Ein Algorithmus zur Berechnung von Ganzheitsbasen in algebraischen Funktionenkörpern

Dissertation
zur Erlangung des Grades
Doktor der Naturwissenschaften
- Dr. rer. nat. -

vorgelegt beim
Fachbereich Mathematik und Informatik
der Universität Duisburg-Essen

von Diplom-Mathematikerin
Elena Mattig
aus Bikin (Rußland)

2003

Vorsitzender:	Prof. Dr. Karl-Josef Witsch, Universität Essen
Erster Gutachter:	Prof. Dr. Henning Stichtenoth, Universität Essen
Zweiter Gutachter:	Prof. Dr. Tom Høholdt, Technical University of Denmark
Tag der mündlichen Prüfung:	25.07.2003

Danksagung

Zu allererst möchte ich mich ganz herzlich bei meinem Betreuer Henning Stichtenoth bedanken für seine ständige Bereitschaft zur Hilfe und zur Beratung, für seine große Geduld und Unterstützung während meiner gesamten Promotionszeit.

Des weiteren möchte ich mich bei Professor Peter Roquette und seiner Frau Erika dafür bedanken, dass es durch ihre Anstrengungen und Mühe für mich möglich geworden ist, in diesem Land meine Doktorarbeit zu schreiben.

Ich bedanke mich bei S. I. Aleschnikov, der mein Interesse an dieser Wissenschaft entstehen ließ und mich in ihr unterrichtet hat.

Ich danke meinen Eltern und meiner Freundin Steffi, die mich in schwierigen Zeiten stets aufgemuntert und gefördert haben.

Inbesondere danke ich meinem geliebten Ehemann Dirk, der die ganze Zeit und in jeder Hinsicht zu mir gestanden hat.

Inhaltsverzeichnis

1 Einleitung

Aus der Kodierungstheorie ist bekannt, dass die Gilbert-Varshamov Schranke (GV-Schranke) die Existenz langer Codes garantiert, deren Güte mindestens diese Schranke erreicht. Man weiß zwar von der Existenz von langen alternanten Codes, die die GV-Schranke erreichen, aber man kennt keine explizite Beschreibung dieser Codes. Im Jahr 1980 hat Goppa [Gop] mit Hilfe der Theorie der algebraischen Kurven eine neue Familie von Codes konstruiert, die heutzutage als algebraisch-geometrische Codes (AG-Codes) bekannt sind. Die Güte eines AG-Codes hängt ab von dem Quotienten N/g der zwei Parameter, die zu einer algebraischen Kurve C über $\mathbb{F}_q$, bzw. zu einem Funktionenkörper $F/\mathbb{F}_q$ gehören. $N = N(C)$ ist die Anzahl der rationalen Punkte auf der Kurve C, bzw. der rationalen Stellen des Funktionenkörpers $F/\mathbb{F}_q$, und g ist das Geschlecht der Kurve C, bzw. des Funktionenkörpers $F/\mathbb{F}_q$. Gute lange AG-Codes bekommt man, wenn N/g groß ist. Die Drinfeld-Vlădut Schranke (DV-Schranke) gibt allerdings eine obere Abschätzung für diesen Quotienten: sei $N_q(g) := max\{\ N(C) \mid C$ ist eine Kurve über $\mathbb{F}_q$ vom Geschlecht $g\}$, dann gilt

$$lim\ sup_{g\to\infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1.$$

Im Jahr 1982 haben Tsfasman, Vlădut und Zink [Tsf-Vla-Zin] die Existenz von Kurven bewiesen, die als modulare Kurven bekannt sind, und deren Quotienten N/g die DV-Schranke asymptotisch erreichen, falls q ein Quadrat ist. Konstruiert man auf solchen Kurven AG-Codes, so haben diese eine große Länge und eine Güte, die in einem gewissen Bereich die GV-Schranke übersteigt. Dies war ein Ergebnis, das man bis zum damaligen Zeitpunkt in der Kodierungstheorie für unerreichbar gehalten hatte. Da Tsfasman, Vlădut und Zink nur die Existenz von solchen Kurven bewiesen hatten, aber keine explizite Darstellung von ihnen angegeben hatten, entstand die Herausforderung, nach expliziten Darstellungen von Kurven zu suchen, auf denen solche Codes konstruiert werden können.

In den Jahren 1995 und 1996 haben Garcia und Stichtenoth [Gar-Sti 1], [Gar-Sti 2] einen wesentlichen Schritt geleistet, indem sie eine explizite Beschreibung zweier Sequenzen von algebraischen Kurven (bzw. Türmen algebraischer Funktionenkörper) angegeben haben, die die DV-Schranke erreichen. Da man für eine explizite Beschreibung eines auf einer dieser Kurven konstruierten AG-Codes eine Basis des Vektorraums $\mathcal{L}(rP_\infty)$ braucht, der sämtliche Funktionen mit genau einem Pol im unendlichen Punkt P_∞ und mit Polordnungen nicht größer als r enthält, entstand die Frage, wie man nun diesen Vektorraum $\mathcal{L}(rP_\infty)$ beschreibt.

Zu diesem Thema sind folgende Arbeiten veröffentlicht worden. Für den in [Gar-Sti 1] konstruierten Turm von Funktionenkörpern $(F_n)_{n\geq 0}$ (dieser wird auch erster Garcia-Stichtenoth Turm (GS-Turm) genannt) wurden explizit die Vektorräume $\mathcal{L}\left(rP^{(n)}\right)$, wobei $P^{(n)}$ eine geeignete rationale Stelle von $F_n/\mathbb{F}_{q^2}$ ist, für F_0, F_1, F_2 in [Vos-Høh] und für F_3 über $\mathbb{F}_{16}$ in [Hac] gefunden. In [Pel-Sti-Tor] haben Pellikaan, Stichtenoth und Torres die Dimension des Vektorraums $\mathcal{L}(rQ)$ bei einer gewissen Wahl der Stelle Q für den in [Gar-Sti 2] beschriebenen Turm von Funktionenkörpern (dieser wird auch zweiter GS-Turm genannt) gefunden. Shany und Be'ery [Sha-Bee] und Aleshnikov, Deolalikar, Kumar und Stichtenoth [Ale-Deo-Kum-Sti] haben nicht zu große Oberräume

$V \supseteq \mathcal{L}\left(rP_\infty^{(n)}\right)$, $P_\infty^{(n)} \in \mathbb{P}_{F_n}$, jeweils für den ersten GS-Turm $(F_n)_{n\geq 0}$ und für den zweiten GS-Turm $(F_n)_{n\geq 0}$ konstruiert. Dafür wurden ähnliche Methoden wie in der algebraischen Zahlentheorie und Eigenschaften von Ganzheitsbasen verwendet. In [Shu-Ale-Kum-Sti-Deo] ist ein Algorithmus zur Berechnung einer Basis des Vektorraums $\bigcup_{r=0}^{q^{n+1}-q^{\lfloor n/2\rfloor+1}+q^n} \mathcal{L}\left(rP_\infty^{(n)}\right)$ für den zweiten GS-Turm $(F_n)_{n\geq 0}$ (über $\mathbb{F}_{q^2}$) mit der Komplexität $O\left((Nlog_qN)^3\right)$, wobei N die Länge des Codes ist, angegeben worden. Leonard [Leo] präsentiert einen iterativen Algorithmus zur Berechnung einer Basis des Rings aller Funktionen aus F_n mit genau einem Pol an der unendlichen Stelle $P_\infty^{(n)}$ für beide GS-Türme $(F_n)_{n\geq 0}$. In [Ale] ist zwar keine Basis für $\mathcal{L}\left(rP_\infty^{(n)}\right)$ für den zweiten GS-Turm explizit berechnet worden, aber es ist eine Methode zu ihrer Berechnung angegeben worden, die Eigenschaften von Basen gewisser Holomorphieringe aus F_n anwendet.

Die Suche nach expliziten Darstellungen von Kurven, bzw. von Funktionenkörpern, deren Quotienten N/g die DV-Schranke erreichen, ging weiter. Im Jahr 1997 haben Garcia, Stichtenoth und Thomas [Gar-Sti-Tho] andere Beispiele von asymptotisch guten Türmen von Funktionenkörpern veröffentlicht. Explizit konstruierte asymptotisch optimale Türme von modularen Kurven hat Elkies im Jahr 1997 in [Elk] präsentiert. Im Jahr 2001 haben Garcia, Stichtenoth und Rück [Gar-Sti-Rüc] noch einen asymptotisch optimalen Turm von Funktionenkörpern konstruiert. Genau so wie für [Gar-Sti 1], [Gar-Sti 2] braucht man für eine explizite Beschreibung eines auf einem der Türme [Gar-Sti-Rüc] oder [Gar-Sti-Tho] konstruierten AG-Codes eine Basis des Vektorraums $\mathcal{L}\left(rP_\infty^{(n)}\right)$.

In meiner Arbeit betrachte ich spezielle Fälle von Funktionenkörpererweiterungen, für die ich ein Verfahren entwickle, mit dem eine Basis des Vektorraums $\mathcal{L}(rP)$, der sämtliche Funktionen mit Polen nur an der Stelle P und Polordnungen nicht größer als r enthält, berechnet werden kann.

Sei F'/F eine endliche separable Funktionenkörpererweiterung mit dem gleichen Konstantenkörper K. Sei $\mathcal{S} \subseteq \mathbb{P}_F$ eine Menge von Stellen des Funktionenkörpers F/K. Wir definieren die folgenden **Holomorphieringe** bezüglich dieser Menge $\mathcal{S}$:

$$\mathcal{O} := \{z \in F \mid v_P(z) \geq 0 \text{ für alle } P \in \mathcal{S}\},$$

$$\mathcal{O}' := \{z \in F' \mid v_{P'}(z) \geq 0 \text{ für alle } P' \in \mathcal{S}'\},$$

wobei $\mathcal{S}' := \{P' \in \mathbb{P}_{F'} \mid P'|P,\ P \in \mathcal{S}\}$. Dann ist der Ring $\mathcal{O}'$ der ganze Abschluss des Ringes $\mathcal{O}$ in F'. Falls $\mathcal{O}$ ein Hauptidealring ist, existiert eine Basis für $\mathcal{O}'$ über $\mathcal{O}$, die eine **Ganzheitsbasis** für $\mathcal{O}'/\mathcal{O}$ genannt wird. Eines der wichtigsten Hilfsmittel meiner Arbeit ist ein neues Kriterium für die Eigenschaft "ein Element aus F' liegt in $\mathcal{O}'$". Damit kann man alle Elemente aus $\mathcal{O}'$ beschreiben und eine Basis für $\mathcal{O}'/\mathcal{O}$ finden.

Ich habe einen Algorithmus zur Berechnung von Ganzheitsbasen für $\mathcal{O}'/\mathcal{O}$ im folgenden Fall entwickelt. Zuerst setze ich voraus, dass $F = \mathbb{F}_q(x)$ ist für ein $x \in F$, welches transzendent über $\mathbb{F}_q$ ist. Dann besitzt x genau einen Pol, der mit P_∞ bezeichnet wird. Daher kann ich $\mathcal{S} = \mathbb{P}_F \setminus \{P_\infty\}$ betrachten. Dann ist $\mathcal{O} = \mathbb{F}_q[x]$ und damit ein Hauptidealring. Jede Ganzheitsbasis für $\mathcal{O}'/\mathcal{O}$ wird in diesem Fall auch eine **Ganzheitsbasis für F'/F** genannt. Falls P_∞ voll verzweigt in F'/F ist, läuft der Algorithmus auf zwei lineare Gleichungssysteme

hinaus, deren Lösungen explizit eine Ganzheitsbasis für F'/F bestimmen. Da in diesem Fall

$$\mathcal{O}' = \bigcup_{r \geq 0}^{\infty} \mathcal{L}\left(rP'_{\infty}\right)$$

gilt, wobei mit $P'_{\infty} \in \mathbb{P}_{F'}$ die einzige Stelle über P_{∞} bezeichnet wird, können Basen für die Vektorräume $\mathcal{L}\left(rP'_{\infty}\right)$ mit Hilfe von Ganzheitsbasen für F'/F bestimmt werden.

Diesen Algorithmus habe ich in der Programmiersprache von Maple 7 für den in [Gar-Sti-Rüc] konstruierten Turm algebraischer Funktionenkörper $(F_n)_{n \geq 0}$ implementiert. Mittels dieses Programms können Basen für die Vektorräume $\mathcal{L}\left(rP_{\infty}^{(n)}\right)$ berechnet werden. Die Komplexität dieses Algorithmus ist mit $O\left(N(F_n)^{19} \cdot log^5 N(F_n) + r\right)$ abgeschätzt, wobei $N(F_n)$ die Anzahl der rationalen Stellen von $F_n/\mathbb{F}_{p^2}$ ist.

Zusätzlich gebe ich ein paar Kummersche Funktionenkörpererweiterungen für Charakteristik gleich 2 mit vielen rationalen Stellen an, von denen zwei eine bessere als bislang bekannte Anzahl der rationalen Stellen liefern.

2 Grundlagen

Einige Definitionen und Ergebnisse aus [Sti] werden in dieser Arbeit häufig benutzt. Wir geben die wichtigsten hier an, um das Lesen der Arbeit zu erleichtern.

2.1 Algebraische Funktionenkörper

In diesem Abschnitt führen wir grundlegende Begriffe und Ergebnisse aus der Funktionenkörpertheorie ein.

Sei K ein Körper und $\bar{K}$ sein algebraischer Abschluß.

Definition 2.1.1 *Ein* **algebraischer Funktionenkörper F/K einer Variablen über K** *(oder einfach algebraischer Funktionenkörper) ist eine Erweiterung $F \supseteq K$, so dass $[F : K(x)] < \infty$ für ein $x \in F$, welches transzendent über K ist. Die Menge $\tilde{K} := \{z \in F \mid z \text{ ist algebraisch über } K\}$ ist ein Unterkörper von F und heißt* **Konstantenkörper** *von F/K. Falls $\tilde{K} = K$, heißt K* **voller Konstantenkörper** *von F/K. Falls $F = K(x)$, heißt F/K* **rationaler Funktionenkörper**.

Sei F/K ein algebraischer Funktionenkörper. Wir werden von nun an der Einfachheit halber stets annehmen, dass K der volle Konstantenkörper von F/K ist.

Definition 2.1.2 *Ein* **Bewertungsring** *des Funktionenkörpers F/K ist ein Ring $\mathcal{O} \subseteq F$, so dass*
(1) $K \subsetneq \mathcal{O} \subsetneq F$, und
(2) $z \in \mathcal{O}$ oder $z^{-1} \in \mathcal{O}$ für alle $z \in F$.
Die Menge $\mathcal{O}^* := \{z \in \mathcal{O} \mid \text{es existiert } w \in \mathcal{O} \text{ mit } zw = 1\}$ heißt die **Einheitengruppe** *von $\mathcal{O}$.*

Proposition 2.1.3 *Sei $\mathcal{O}$ ein Bewertungsring des Funktionenkörpers F/K. Dann gilt:*
(1) $\mathcal{O}$ ist ein lokaler Ring, d.h. $\mathcal{O}$ besitzt genau ein maximales Ideal $P = \mathcal{O} \setminus \mathcal{O}^*$.
(2) $\mathcal{O}$ ist ein Hauptidealring.

Definition 2.1.4 *Das maximale Ideal eines Bewertungsringes $\mathcal{O} \subset F$ heißt* **Stelle** *des Funktionenkörpers F/K. Die Menge*

$$\mathbb{P}_F := \{P \mid P \text{ ist eine Stelle von } F/K\}$$

ist die Menge aller Stellen von F/K. Wir bezeichnen mit $\mathcal{O}_P$ den eindeutig bestimmten Bewertungsring von F/K, dessen maximales Ideal P ist.

Sei $P \in \mathbb{P}_F$ eine Stelle von F/K.

Definition 2.1.5 *Ein Element $t \in P$ mit $P = t\mathcal{O}_P$ heißt ein* **Primelement** *von P. $F_P := \mathcal{O}_P/P$ heißt der* **Restklassenkörper** *von P. Wir schreiben:*

$$\begin{aligned} x(P) &:= x + P \in F_P, && \text{falls } x \in \mathcal{O}_P, \\ x(P) &:= \infty, && \text{falls } x \in F \setminus \mathcal{O}_P. \end{aligned}$$

Der **Grad der Stelle** *P ist definiert als $\deg P := [F_P : K]$. Die Stelle P heißt* **rationale Stelle**, *falls $\deg P = 1$.*

Bemerkung 2.1.6 *Falls $P \in \mathbb{P}_F$ eine rationale Stelle ist, folgt $F_P = K$. Insbesondere, falls K algebraisch abgeschlossen ist, sind alle Stellen von F/K rational.*

Für die weiteren Beschreibungen von Bewertungsringen und Stellen von Funktionenkörpern brauchen wir den Begriff der diskreten Bewertung.

Definition 2.1.7 *Eine* **diskrete Bewertung** *von F/K ist eine Funktion $v : F \to \mathbb{Z} \cup \{\infty\}$ mit den folgenden Eigenschaften:*
(1) $v(x) = \infty \iff x = 0$,
(2) $v(xy) = v(x) + v(y)$ für alle $x, y \in F$,
(3) $v(x + y) \geq min\{v(x), v(y)\}$ für alle $x, y \in F$,
(4) $v(a) = 0$ für alle $0 \neq a \in K$,
(5) Es existiert ein $z \in F$ mit $v(z) = 1$.

Lemma 2.1.8 *Sei v eine diskrete Bewertung von F/K und $x, y \in F$ mit $v(x) \neq v(y)$. Dann gilt $v(x + y) = min\{v(x), v(y)\}$.*

Definition 2.1.9 *Für $P \in \mathbb{P}_F$ bezeichnen wir mit v_P die wie folgt definierte Funktion: wir wählen ein Primelement $t \in P$. Dann hat jedes $0 \neq z \in F$ eine eindeutige Darstellung $z = t^n u$ mit $u \in \mathcal{O}_P^*$ und $n \in \mathbb{Z}$. Wir definieren*

$$v_P(z) := n \text{ und } v_P(0) := \infty.$$

Theorem 2.1.10 *Sei F/K ein Funktionenkörper. Für jede Stelle $P \in \mathbb{P}_F$ ist die Funktion v_P eine diskrete Bewertung von F/K. Außerdem gilt:*

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\},$$

$$\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\},$$

$$P = \{z \in F \mid v_P(z) > 0\}.$$

Ein Element $t \in F$ ist ein Primelement von P dann und nur dann, wenn $v_P(t) = 1$.

Definition 2.1.11 *Sei $z \in F$. P ist eine* **Nullstelle** *von z dann und nur dann, wenn $v_P(z) > 0$. P ist ein* **Pol** *von z dann und nur dann, wenn $v_P(z) < 0$. Falls P ein Pol von z ist, dann heißt die Zahl $n = -v_P(z)$* **Polordnung** *von z an der Stelle P.*

Lemma 2.1.12 *Sei $z \in F$ transzendent über K. Dann besitzt z mindestens eine Nullstelle und mindestens einen Pol. Daher gilt insbesondere $\mathbb{P}_F \neq \emptyset$.*

Wir werden häufig mit einem rationalen Funktionenkörper arbeiten, deshalb geben wir hierfür einige Begriffe und Definitionen an.

Definition 2.1.13 *Sei $K(x)/K$ ein rationaler Funktionenkörper. Ist ein beliebiges normiertes irreduzibles Polynom $p(x) \in K[x]$ gegeben, so betrachten wir den Bewertungsring*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\}$$

von $K(x)/K$ mit seinem maximalen Ideal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ p(x) \mid f(x),\ p(x) \nmid g(x) \right\}.$$

Es existiert ein weiterer Bewertungsring von $K(x)/K$, nämlich

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ deg\ f(x) \leq deg\ g(x) \right\}$$

mit seinem maximalen Ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ deg\ f(x) < deg\ g(x) \right\}.$$

P_∞ heißt die **unendliche Stelle** *von $K(x)/K$.*

Theorem 2.1.14 *Es existieren keine anderen Stellen von $K(x)/K$ außer den Stellen $P_{p(x)}$ und P_∞, die per Definition 2.1.13 definiert sind.*

Im folgenden führen wir einige weitere Begriffe ein.

Definition 2.1.15 *Die von allen Stellen des Funktionenkörpers F/K erzeugte frei abelsche Gruppe $\boldsymbol{\mathcal{D}_F}$ heißt die* **Divisorengruppe** *von F/K. Ein* **Divisor** *ist also eine formale Summe*

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ mit } n_P \in \mathbb{Z},\ \text{fast alle } n_P = 0.$$

Für $Q \in \mathbb{P}_F$ definieren wir $v_Q(D) := n_Q$.
Der **Träger** *des Divisors D ist definiert als*

$$supp\ D := \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}.$$

Der **Grad des Divisors** *D ist definiert als*

$$deg\ D := \sum_{P \in supp\ D} v_P(D) deg\ P.$$

Eine partielle Ordnung auf $\mathcal{D}_F$ ist definiert durch

$$D_1 \leq D_2 :\Longleftrightarrow v_P(D_1) \leq v_P(D_2) \text{ für alle } P \in \mathbb{P}_F.$$

Definition 2.1.16 *Sei $0 \neq x \in F$. Sei Z_1 die Menge aller Pole und Z_2 die Menge aller Nullstellen von x in $\mathbb{P}_F$. Dann definieren wir*

$$(x)_\infty := \sum_{P \in Z_1} (-v_P(x))P \text{ als } \textbf{Poldivisor} \text{ von } x,$$

$$(x)_0 := \sum_{P \in Z_2} v_P(x)P \text{ als } \textbf{Nulldivisor} \text{ von } x,$$

$$(x) := (x)_0 - (x)_\infty \text{ als } \textbf{Hauptdivisor} \text{ von } x.$$

Definition 2.1.17 *Für einen Divisor $A \in \mathcal{D}_F$ sind der mit ihm assoziierte K-Vektorraum* $\boldsymbol{\mathcal{L}(A)}$ *und seine* **Dimension** *wie folgt definiert:*

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\},$$

$$dim\ A := dim_K\ \mathcal{L}(A).$$

Nach Definition von $\mathcal{L}(A)$ gilt also:

Lemma 2.1.18 *Sei $A \in \mathcal{D}_F$. Dann gilt:*

$$x \in \mathcal{L}(A) \Longleftrightarrow v_P(x) \geq -v_P(A) \text{ für alle } P \in \mathbb{P}_F.$$

Definition 2.1.19 *Das* **Geschlecht** *von F/K ist definiert als*

$$g := max\{deg\ A - dim\ A + 1 \mid A \in \mathcal{D}_F\}.$$

Definition 2.1.20 *Eine Zahl $n \in \mathbb{N} \cup \{0\}$ heißt* **Polzahl** *von P dann und nur dann, falls ein $x \in F$ mit $(x)_\infty = nP$ existiert. Falls $n \in \mathbb{N}$ keine Polzahl von P ist, heißt sie* **Fehlzahl** *von P.*

Theorem 2.1.21 *Sei F/K vom Geschlecht $g > 0$ und P eine rationale Stelle. Dann existieren genau g Fehlzahlen $i_1 < \ldots < i_g$ von P, und es gilt*

$$i_1 = 1 \text{ und } i_g \leq 2g - 1.$$

Der Hauptteil dieser Arbeit basiert auf dem sogenannten Ganzheitskriterium (Proposition 3.3.1), für das folgende Definitionen und Ergebnisse eine wichtige Rolle spielen.

Definition 2.1.22 *Für $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$ sei*

$$\mathcal{O}_\mathcal{S} := \{z \in F \mid v_P(z) \geq 0 \text{ für alle } P \in \mathcal{S}\}$$

der Durchschnitt aller Bewertungsringe $\mathcal{O}_P$ mit $P \in \mathcal{S}$. $\mathcal{O}_\mathcal{S}$ heißt ein **Holomorphiering** *von F/K.*

Definition 2.1.23 *Sei $R \subset F$ ein Ring. Ein Element $z \in F$ heißt* **ganz über** *R, falls ein normiertes Polynom $f(X) \in R[X]$ mit $f(z) = 0$ existiert. Die Menge*

$$ic_F(R) := \{z \in F \mid z \text{ ist ganz über } R\}$$

heißt der **ganze Abschluß** *von R in F. Falls F der Quotientenkörper von R ist und $ic_F(R) = R$ gilt, heißt R* **ganz abgeschlossen**.

Proposition 2.1.24 *Sei $\mathcal{O}_\mathcal{S}$ ein Holomorphiering von F/K. Dann gilt:*
(1) F ist der Quotientenkörper von $\mathcal{O}_\mathcal{S}$.
(2) $\mathcal{O}_\mathcal{S}$ ist ganz abgeschlossen.

Proposition 2.1.25 *Falls $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$ endlich ist, ist $\mathcal{O}_\mathcal{S}$ ein Hauptidealring. Sei $P \in \mathbb{P}_F$ und $\mathcal{S} = \mathbb{P}_F \setminus \{P\}$, dann gilt $\mathcal{O}_\mathcal{S} = \bigcup_{r \geq 0}^{\infty} \mathcal{L}(rP)$.*

2.2 Erweiterungen algebraischer Funktionenkörper

In diesem Abschnitt werden grundlegende Begriffe und Ergebnisse über Körpererweiterungen von Funktionenkörpern eingeführt.

Sei F/K ein Funktionenkörper, wobei K der volle Konstantenkörper von F/K ist. Sei $K' \supseteq K$ eine algebraische Erweiterung.

Definition 2.2.1 *Ein algebraischer Funktionenkörper F'/K' heißt eine* **algebraische Funktionenkörpererweiterung** *von F/K, falls $F' \supseteq F$ eine algebraische Körpererweiterung ist mit $K' \supseteq K$. Wir bezeichnen sie im folgenden mit $\boldsymbol{F'/F}$. Die algebraische Funktionenkörpererweiterung F'/F heißt* **endlich**, *falls $[F' : F] < \infty$.*

Definition 2.2.2 *Eine algebraische Funktionenkörpererweiterung F'/F heißt eine* **Konstantenkörpererweiterung**, *wenn $F' = FK'$, das Kompositum von F und K' ist.*

Sei F'/F eine algebraische Funktionenkörpererweiterung. Sei $P' \in \mathbb{P}_{F'}$ und $P \in \mathbb{P}_F$.

Definition 2.2.3 *Die Stelle P'* **liegt über** *P, falls $P' \supseteq P$. Mit anderen Worten, P' ist eine* **Fortsetzung** *von P, und wir schreiben $P'|P$.*

Proposition 2.2.4 *Für jede Stelle $P' \in \mathbb{P}_{F'}$ existiert genau eine Stelle $P \in \mathbb{P}_F$, so dass $P'|P$. Umgekehrt besitzt jede Stelle $P \in \mathbb{P}_F$ mindestens eine, aber nur endlich viele Fortsetzungen $P' \in \mathbb{P}_{F'}$.*

Proposition 2.2.5 *Die drei folgenden Aussagen sind äquivalent:*
(1) $P'|P$.
(2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.
(3) Es existiert ein $e \in \mathbb{N}$ mit $e \geq 1$, so dass $v_{P'}(x) = e \cdot v_P(x)$ für alle $0 \neq x \in F$.
Insbesondere gilt für $P'|P$:

$$P = P' \cap F \text{ und } \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

Definition 2.2.6 *Sei e wie in Proposition 2.2.5. Die Zahl $e(P'|P) := e$ mit*

$$v_{P'}(x) = e(P'|P) \cdot v_P(x)$$

für alle $0 \neq x \in F$ heißt der **Verzweigungsindex** *von P' über P. Die Zahl $f(P'|P) := [F'_{P'} : F_P]$ heißt der* **relative Grad** *von P' über P.*

Definition 2.2.7 *Die Fortsetzung $P'|P$ heißt*
(1) **verzweigt**, *falls $e(P'|P) > 1$ ist.*
(2) **unverzweigt**, *falls $e(P'|P) = 1$ ist.*
Die Stelle P heißt
(3) **verzweigt** *in F'/F, falls eine Stelle $P' \in \mathbb{P}_{F'}$ existiert, die über P liegt, so dass $P'|P$ verzweigt ist.*
(4) **voll verzweigt** *in F'/F, falls genau eine Stelle $P' \in \mathbb{P}_{F'}$ existiert, die über P liegt, und $e(P'|P) = [F' : F]$.*
(5) **voll zerlegt** *in F'/F, falls die Anzahl der Fortsetzungen von P gleich $[F' : F]$ ist.*

Im Allgemeinen hängen der Verzweigungsindex und der relative Grad von $P'|P$ nicht nur von P ab, sondern auch von der Wahl der Fortsetzung P' von P in F'. Allerdings hat man im Fall einer galoisschen Erweiterung folgendes:

Theorem 2.2.8 *Sei F'/F galoissch. Seien $P_1, \ldots, P_n \in \mathbb{P}_{F'}$ alle Stellen, die über $P \in \mathbb{P}_F$ liegen. Dann gilt:*
(1) $e(P_i|P) = e(P_j|P)$ und $f(P_i|P) = f(P_j|P)$ für $i, j = 1, \ldots, n$. Wir setzen

$$e(P) := e(P_i|P) \text{ und } f(P) := f(P_i|P)$$

und nennen $e(P)$ den **Verzweigungsindex** *und $f(P)$ den* **relativen Grad** *von P in F'/F.*
(2) $e(P) \cdot f(P) \cdot n = [F' : F]$.

Proposition 2.2.9 *Sei F''/K'' eine algebraische Erweiterung von F'/K', und liege $P'' \in \mathbb{P}_{F''}$ über P'. Dann gilt:*

$$e(P''|P) = e(P''|P') \cdot e(P'|P),$$

$$f(P''|P) = f(P''|P') \cdot f(P'|P).$$

Proposition 2.2.10 *Sei K vollkommen und $F' = FK'$ eine algebraische Konstantenkörpererweiterung von F/K. Dann gilt:*
(1) $[F : K(x)] = [F' : K'(x)]$ für alle $x \in F \setminus K$.
(2) K' ist der volle Konstantenkörper von F'.
(3) $P'|P$ ist unverzweigt in F'/F für alle $P \in \mathbb{P}_F$ und für alle $P' \in \mathbb{P}_{F'}$ mit $P'|P$.
(4) F'/K' hat das gleiche Geschlecht wie F/K.

Proposition 2.2.11 (Abhyankar's Lemma) *Sei F'/F eine endliche separable Funktionenkörpererweiterung und $F' = F_1F_2$ das Kompositum zweier Zwischenkörper $F \subseteq F_1, F_2 \subseteq F'$. Sei $P' \in \mathbb{P}_{F'}$ eine Fortsetzung von $P \in \mathbb{P}_F$, und wir setzen $P_i := P' \cap F_i$ für $i = 1, 2$. Falls mindestens einer der Verzweigungsindizes $e(P_1|P)$ oder $e(P_2|P)$ teilerfremd zur Charakteristik von F ist, gilt*

$$e(P'|P) = kgV(e(P_1|P), e(P_2|P)).$$

Die nächsten Propositionen und das folgende Theorem bilden den Ausgangspunkt für eine Methode, um Ganzheitsbasen zu finden, die als Fundament für diese Arbeit dient.

Proposition 2.2.12 *Sei M/L eine endliche separable Körpererweiterung und $\{z_1, \ldots, z_n\}$ eine Basis von M/L. Dann existieren eindeutig bestimmte Elemente $z_1^*, \ldots, z_n^* \in M$, so dass*

$$Tr_{M/L}(z_i z_j^*) = \delta_{ij}$$

gilt, wobei $Tr_{M/L} : M \to L$ die Spurabbildung und δ_{ij} das Kroneckersymbol sind. Die Menge $\{z_1^*, \ldots, z_n^*\}$ ist eine Basis von M/L und heißt die **duale Basis** *von $\{z_1, \ldots, z_n\}$ (bezüglich der Spurabbildung).*

Theorem 2.2.13 *Sei $R \subset F$ ein ganz abgeschlossener Ring mit dem Quotientenkörper F und F'/F eine endliche separable Funktionenkörpererweiterung vom Grad n. Sei $R' := ic_{F'}(R)$. Dann gelten folgende Aussagen:*
(1) Für jede Basis $\{x_1, \ldots, x_n\}$ für F'/F existieren Elemente $a_i \in R \setminus \{0\}$ für $i = 1, \ldots, n$, so dass $a_1 x_1, \ldots, a_n x_n \in R'$. Daher existieren Basen für F'/F mit Elementen aus R'.
(2) Falls $\{z_1, \ldots, z_n\} \subseteq R'$ eine Basis für F'/F und $\{z_1^*, \ldots, z_n^*\}$ ihre duale Basis ist, gilt:

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$

(3) Sei R ein Hauptidealring. Dann existiert eine Basis $\{u_1, \ldots, u_n\}$ für F'/F, so dass $R' = \sum_{i=1}^{n} Ru_i$ gilt.

Proposition 2.2.14 *Sei F'/F eine endliche separable Funktionenkörpererweiterung vom Grad n und $P \in \mathbb{P}_F$. Dann ist der ganze Abschluß von $\mathcal{O}_P$ in F'*

$$ic_{F'}(\mathcal{O}_P) = \bigcap_{P'|P} \mathcal{O}_{P'},$$

und es existiert eine Basis $\{u_1, \ldots, u_n\}$ für F'/F, so dass

$$ic_{F'}(\mathcal{O}_P) = \sum_{i=1}^{n} \mathcal{O}_P u_i.$$

Definition 2.2.15 *Die in Proposition 2.2.14 beschriebene Basis heißt eine* **Ganzheitsbasis** *für $ic_{F'}(\mathcal{O}_P)$ über $\mathcal{O}_P$ und heißt eine* **lokale Ganzheitsbasis** *für F'/F an der Stelle P.*

Lemma 2.2.16 *Sei F'/F eine endliche separable Funktionenkörpererweiterung vom Grad n und $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$. Dann ist $\{u_1, \ldots, u_n\}$ eine Ganzheitsbasis für $ic_{F'}\left(\bigcap_{P \in \mathcal{S}} \mathcal{O}_P\right)$ über $\bigcap_{P \in \mathcal{S}} \mathcal{O}_P$ genau dann, wenn sie eine Ganzheitsbasis für $ic_{F'}(\mathcal{O}_P)$ über $\mathcal{O}_P$ für alle $P \in \mathcal{S}$ ist.*

Im Kapitel 5 werden Funktionenkörpererweiterungen mit vielen rationalen Stellen angegeben, deren Struktur in der nächsten Proposition beschrieben wird.

Proposition 2.2.17 *Sei F/K ein algebraischer Funktionenkörper, wobei K eine primitive n-te Einheitswurzel enthält (mit $n > 1$ und $ggT(n, Char\ K) = 1$). Sei $u \in F$ mit*

$$u \neq w^d \text{ für alle } w \in F \text{ und alle } d \mid n, d > 1.$$

Weiterhin sei

$$F' := F(y) \text{ mit } y^n = u.$$

Die Funktionenkörpererweiterung F'/F heißt **Kummersche Erweiterung** *von F. Es gilt:*
(1) Das Polynom $X^n - u$ ist das Minimalpolynom von y über F, und die Erweiterung F'/F ist galoissch vom Grad n.
(2) Sei $P \in \mathbb{P}_F$ und $P' \in \mathbb{P}_{F'}$ mit $P'|P$. Dann gilt:

$$e(P'|P) = \frac{n}{r_P} \text{ mit } r_P := ggT(n, v_P(u)) > 0.$$

(3) Sei K' der Konstantenkörper von F' und g (bzw. g') das Geschlecht von F/K (bzw. von F'/K'). Dann gilt:

$$g' = 1 + \frac{n}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) deg\ P \right).$$

Folgerung 2.2.18 *Sei F/K ein Funktionenkörper und sei $F' = F(y)$ mit $y^n = u \in F$, wobei $n \not\equiv 0$ mod Char K, und K enthält eine primitive n-te Einheitswurzel. Existiert eine Stelle $Q \in \mathbb{P}_F$ mit $ggT(v_Q(u), n) = 1$, dann ist K der volle Konstantenkörper von F', und es gilt:*

$$g' = 1 + n(g-1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) deg\ P.$$

2.3 Türme algebraischer Funktionenkörper

Eine andere Art von Funktionenkörpererweiterungen ist ein Turm. Die folgenden Definitionen, sowie einige Beispiele für Türme kann man in [Gar-Sti 1], [Gar-Sti 2], [Gar-Sti-Rüc], [Gar-Sti-Tho] und [Tho] finden.

Sei K ein Körper.

Definition 2.3.1 *Eine Folge $\mathcal{F} = (F_0, F_1, \ldots)$ von Funktionenkörpern F_i/K heißt ein* **Funktionenkörperturm** *über K, falls*
(1) $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n \subseteq \ldots$
(2) F_n/F_{n-1} ist separabel vom Grad $[F_n : F_{n-1}] > 1$ für alle $n > 0$.
(3) $g(F_n) > 1$ für ein $n \geq 0$.

Sei $\mathcal{F}$ ein Funktionenkörperturm über K und $P \in \mathbb{P}_{F_0}$.

Definition 2.3.2 *Die Stelle P heißt*
(1) **unverzweigt in $\mathcal{F}$**, *falls P in keiner Erweiterung F_n/F_0 verzweigt ist.*
(2) **verzweigt in $\mathcal{F}$**, *falls ein $n \in \mathbb{N}$ exisitert, so dass P in F_n/F_0 verzweigt ist.*
(3) **voll verzweigt in $\mathcal{F}$**, *falls P in jeder Erweiterung F_n/F_0 voll verzweigt ist.*

Definition 2.3.3 *Der* **Verzweigungsort** *von $\mathcal{F}$ ist die Menge*

$$V(\mathcal{F}) := \{P \in \mathbb{P}_{F_0} \mid P \text{ ist verzweigt in } \mathcal{F}\}.$$

3 Basen für die Vektorräume $\mathcal{L}\left(rP'_\infty\right)$

In diesem Kapitel wird ein Algorithmus entwickelt, mittels dessen Ganzheitsbasen für endliche separable Funktionenkörpererweiterungen $F'/\mathbb{F}_q(x)$ vom Grad m, wobei die unendliche Stelle $P_\infty \in \mathbb{P}_{\mathbb{F}_q(x)}$ voll verzweigt in $F'/\mathbb{F}_q(x)$ ist, explizit berechnet werden können. Hat eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ modulo m paarweise inkongruente Polordnungen an der Stelle $P'_\infty \in \mathbb{P}_{F'}$ mit $P'_\infty|P_\infty$, so ist der Vektorraum $\mathcal{L}\left(rP'_\infty\right)$ leicht zu beschreiben.

3.1 Vorbereitungen

Sei F'/F eine endliche separable Funktionenkörpererweiterung vom Grad m mit gleichem perfektem Konstantenkörper K. Sei $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$ eine Menge von Stellen des Funktionenkörpers F/K.

(1) Wir fixieren die folgenden Holomorphieringe bezüglich der Menge $\mathcal{S}$:

$$\mathcal{O} := \{z \in F \mid v_P(z) \geq 0 \text{ für alle } P \in \mathcal{S}\} = \bigcap_{P \in \mathcal{S}} \mathcal{O}_P \subseteq F,$$

$$\mathcal{O}' := \{z \in F' \mid v_{P'}(z) \geq 0 \text{ für alle } P' \in \mathcal{S}'\} = \bigcap_{P' \in \mathcal{S}'} \mathcal{O}_{P'} \subseteq F',$$

wobei $\mathcal{S}' := \{P' \in \mathbb{P}_{F'} \mid P'|P,\ P \in \mathcal{S}\}$. Nach 2.2.14 gilt $\mathcal{O}' = ic_{F'}(\mathcal{O})$.

(2) Wir wählen eine Basis $\{w_1, \ldots, w_m\}$ für F'/F mit der Eigenschaft

$$\mathcal{O}' \subseteq \sum_{i=1}^{m} \mathcal{O} w_i.$$

Solche Basen existieren tatsächlich, dies folgt aus Theorem 2.2.13(2). Wir nehmen an, dass

$$v_{P'}(w_i) < 0$$

für mindestens ein $i \in \{1, \ldots, m\}$ und für eine Stelle $P' \in \mathcal{S}'$ gilt.[1]

(3) Wir definieren die Menge M:

$$M := \sum_{i=1}^{m} \mathcal{O} w_i \supseteq \mathcal{O}'.$$

Nach Konstruktion ist M ein endlich erzeugter $\mathcal{O}$-Modul.

(4) Wir wählen eine Zahl $Q \in \mathbb{N}$ mit $v_{P'}(w_i) > -Q$ für $i = 1, \ldots, m$ und für alle $P' \in \mathcal{S}'$. Da alle $w_i \neq 0$, gibt es nur endlich viele Stellen $P' \in \mathcal{S}'$, die Pol eines der Elemente $w_1, \ldots, w_m$ sind. Wählen wir Q größer als alle diese Polordnungen, so hat Q offenbar die gewünschte Eigenschaft.

[1] Sonst wäre $w_i \in \mathcal{O}'$ für $i = 1, \ldots, m$, und damit würde dann $\sum_{i=1}^{m} \mathcal{O} w_i \subseteq \mathcal{O}'$ folgen. Dies würde bedeuten $\mathcal{O}' = \sum_{i=1}^{m} \mathcal{O} w_i$, und damit hätten wir gleich eine Ganzheitsbasis für F'/F als Basis $\{w_1, \ldots, w_m\}$ gefunden.

3.2 Ganzheitsbasen für Holomorphieringe in einer endlichen separablen Funktionenkörpererweiterung

Als ein Hilfsmittel für den oben erwähnten Algorithmus zur Berechnung von Ganzheitsbasen für $F'/\mathbb{F}_q(x)$ benötigen wir den Beweis von Theorem 2.2.13(3). Daher geben wir diesen hier nochmal an.

Seien $w_1, \ldots, w_m$ und M wie in Abschnitt 3.1 gegeben.

Theorem 3.2.1 *Sei $\mathcal{O}$ ein Hauptidealring. Dann existiert eine Basis $\{u_1, \ldots, u_m\}$ für F'/F mit der Eigenschaft*

$$\mathcal{O}' = \sum_{i=1}^{m} \mathcal{O}u_i.$$

Beweis. Für $1 \leq k \leq m$ definieren wir:

$$R_k := \mathcal{O}' \cap \sum_{i=1}^{k} \mathcal{O}w_i. \tag{1}$$

Wir werden $u_1, \ldots, u_m \in \mathcal{O}'$ finden, so dass $R_k = \sum_{i=1}^{k} \mathcal{O}u_i$ für $k = 1, \ldots, m$ gilt. Daraus folgt dann

$$\sum_{i=1}^{m} \mathcal{O}u_i = R_m = \mathcal{O}' \cap M = \mathcal{O}'.$$

Wir zeigen dies durch Induktion nach k.

Für $k = 1$ gilt $R_1 = \mathcal{O}' \cap \mathcal{O}w_1$. Sei $I_1 := \{a \in F \mid aw_1 \in \mathcal{O}'\}$. Es ist klar, dass I_1 ein Ideal in $\mathcal{O}$ ist, und da $\mathcal{O}$ ein Hauptidealring ist, existiert ein $c_{(1,1)} \in \mathcal{O}$ mit $< c_{(1,1)} >= I_1$. Wir setzen $u_1 := c_{(1,1)}w_1$, und damit ist $R_1 = \mathcal{O}u_1$.

Mit der Induktionsannahme für $k-1$ gilt für $k \geq 2$: $u_1, \ldots, u_{k-1}$ sind schon gefunden worden, und $R_{k-1} = \sum_{i=1}^{k-1} \mathcal{O}u_i$.

Wir zeigen den Schritt $k-1 \to k$. Sei

$$I_k := \{a_k \in F \mid \text{es existieren } a_1, \ldots, a_{k-1} \in \mathcal{O}, \text{ so dass } \sum_{i=1}^{k} a_i w_i \in \mathcal{O}'\}.$$

Dann ist I_k auch ein Ideal in $\mathcal{O}$, und damit ist $I_k =< c_{(k,k)} >$ für ein $c_{(k,k)} \in \mathcal{O}$. Wir wählen ein $u_k \in \mathcal{O}'$, so dass

$$u_k = \sum_{i=1}^{k} c_{(i,k)} w_i$$

für gewisse $c_{(i,k)} \in \mathcal{O}$ für $i = 1, \ldots, k-1$. Wegen (1) folgt $\sum_{i=1}^{k} \mathcal{O}u_i \subseteq R_k$.

Nun zeigen wir die inverse Inklusion. Sei $w \in R_k$. Dann gilt $w = \sum_{i=1}^{k} d_i w_i$ mit $d_i \in \mathcal{O}$. Damit ist $d_k \in I_k$ und $d_k = dc_{(k,k)}$ mit $d \in \mathcal{O}$. Daraus folgt aber:

$$w - du_k \in \mathcal{O}' \cap \sum_{i=1}^{k-1} \mathcal{O}w_i = R_{k-1} = \sum_{i=1}^{k-1} \mathcal{O}u_i.$$

Damit haben wir $w \in \sum_{i=1}^{k} \mathcal{O}u_i$.

Wir haben gezeigt, dass $\mathcal{O}' = \sum_{i=1}^{m} \mathcal{O}u_i$. Da $\mathcal{O}'$ nach Theorem 2.2.13(1) eine Basis für F'/F enthält, sind die Elemente $u_1, \ldots, u_m$ linear unabhängig über F und bilden daher eine Basis für F'/F.

□

3.3 Ein Ganzheitskriterium

Nach dem Beweis von Theorem 3.2.1 wissen wir: beschreiben wir die Ideale $I_k \lhd \mathcal{O}$ für $k = 1, \ldots, m$, und finden wir ihre Erzeuger $c_{(k,k)}$, so bestimmen wir Ganzheitsbasiselemente u_1 und u_k für $k = 2, \ldots, m$ bei einer gewissen Wahl von $c_{(i,k)}$ für $i = 1, \ldots, k-1$. Nach Konstruktion von I_k gilt:

$$\sum_{i=1}^{k} a_i w_i \in \mathcal{O}'$$

für jedes $a_k \in I_k$ und für gewisse $a_i \in \mathcal{O}$ für $i = 1, \ldots, k-1$, falls $k \geq 2$ ist. Daher stellt sich die Frage, wann überhaupt ein Element aus dem Funktionenkörper F' in $\mathcal{O}'$ liegt.

Seien $w_1, \ldots, w_m$, M und Q wie in Abschnitt 3.1 gegeben.

Proposition 3.3.1 *Sei $z \in F'$. Dann gilt: $z \in \mathcal{O}' \iff z \in M$ und $z^Q \in M$.*

Beweis.
$\Longrightarrow$ $z \in \mathcal{O}' \Rightarrow z^Q \in \mathcal{O}'$, da $\mathcal{O}'$ ein Ring ist, und es gilt $z \in M$ und $z^Q \in M$, da $\mathcal{O}' \subseteq M$ ist.
$\Longleftarrow$ Nach Konstruktion von M hat z^Q die Gestalt

$$z^Q = \sum_{i=1}^{m} r_i w_i$$

mit $r_i \in \mathcal{O}$ für $i = 1, \ldots, m$. Dann gilt für alle $P' \in \mathcal{S}'$:

$$v_{P'}\left(z^Q\right) = v_{P'}\left(\sum_{i=1}^{m} r_i w_i\right) \geq min_i\{v_{P'}(r_i w_i)\} \geq min_i\{v_{P'}(w_i)\} > -Q.$$

Andererseits gilt

$$v_{P'}\left(z^Q\right) = Q v_{P'}(z).$$

Daraus folgt $Q v_{P'}(z) > -Q \Longrightarrow v_{P'}(z) \geq 0$ für alle $P' \in \mathcal{S}'$. Damit ist $z \in \mathcal{O}'$.

□

3.4 Ganzheitsbasen für $F'/\mathbb{F}_q(x)$

Gelten die Voraussetzungen aus Abschnitt 3.1. Sei $F = \mathbb{F}_q(x)$, wobei $\mathbb{F}_q$ der endliche Körper mit $q = p^n$ Elementen und Char $\mathbb{F}_q = p$ ist. Dann besitzt x genau einen Pol in $\mathbb{F}_q(x)$, den wir mit P_∞ bezeichnen. Sei P_∞ voll verzweigt in $F'/\mathbb{F}_q(x)$. Sei $P'_\infty \in \mathbb{P}_{F'}$ mit $P'_\infty | P_\infty$. Sei $\mathcal{S} = \mathbb{P}_{\mathbb{F}_q(x)} \setminus \{P_\infty\}$, und damit ist $\mathcal{S}' = \mathbb{P}_{F'} \setminus \{P'_\infty\}$. Eine Ganzheitsbasis für $\mathcal{O}'/\mathcal{O}$ wird in diesem Fall eine **(globale) Ganzheitsbasis** *für $F'/\mathbb{F}_q(x)$ genannt.*

Da wir jetzt mit einem rationalen Funktionenkörper arbeiten, wird jedes maximale Ideal in einem Bewertungsring (außer $\mathcal{O}_\infty$) von $\mathbb{F}_q(x)$ erzeugt durch ein normiertes, irreduzibles Polynom aus $\mathbb{F}_q[x]$. Daher hat jede Stelle (außer P_∞) von $\mathbb{F}_q(x)/\mathbb{F}_q$ diese Gestalt, d.h. $P = (p(x))$ für ein normiertes, irreduzibles Polynom $p(x) \in \mathbb{F}_q[x]$. Nach Theorem 2.1.14 existiert eine 1:1 Beziehung zwischen den Stellen in $\mathcal{S}$ und den normierten, irreduziblen Polynomen aus $\mathbb{F}_q[x]$.

Damit sieht der Holomorphiering $\mathcal{O}$ in diesem Fall wie folgt aus:

$$\mathcal{O} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}_q[x],\ p(x) \nmid g(x) \text{ für alle } P = (p(x)) \in \mathcal{S} \right\} = \mathbb{F}_q[x].$$

Seien $w_1, \ldots, w_m$, Q und M wie in Abschnitt 3.1 gegeben.

Da $\{w_1, \ldots, w_m\}$ eine Basis für $F'/\mathbb{F}_q(x)$ ist, gilt für $i = 1, \ldots, m$:

$$w_i^Q = \sum_{j=1}^{m} b_{ij} w_j, \tag{2}$$

mit

$$b_{ij} = \frac{b'_{ij}}{d_{ij}} \in \mathbb{F}_q(x), \tag{3}$$

wobei $b'_{ij}, d_{ij} \in \mathbb{F}_q[x]$ teilerfremd sind.

Bemerkung 3.4.1 *Falls für alle $i, j = 1, \ldots, m$ $d_{ij} = 1$ gilt, folgt, dass die Basis $\{w_1, \ldots, w_m\}$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ ist. Wegen (2) gilt nämlich $w_i^Q \in M$ für $i = 1, \ldots, m$, und nach Proposition 3.3.1 ist dann $w_i \in \mathcal{O}'$ für $i = 1, \ldots, m$. Damit folgt $M \subseteq \mathcal{O}'$, und nach Konstruktion von M ist $\mathcal{O}' \subseteq M$, so dass*

$$\mathcal{O}' = M = \sum_{i=1}^{m} \mathcal{O} w_i.$$

Für die folgenden Berechnungen nehmen wir daher an, dass ein Tupel $(i, j) \in \{1, \ldots, m\}^2$ existiert mit $d_{ij} \neq 1$.

Wir setzen für $i = 1, \ldots, m$

$$d_i := kgV(d_{i1}, \ldots, d_{im}).$$

Das Polynom d_i läßt sich (bis auf die Reihenfolge der Faktoren) eindeutig als Produkt von Potenzen irreduzibler Polynome schreiben. Seien $f_{1i}, \ldots, f_{t_i i}$ für ein $t_i \in \mathbb{N}$ die irreduziblen Polynome aus $\mathbb{F}_q[x]$, so dass

$$d_i = \prod_{s=1}^{t_i} f_{si}^{g_{si}}$$

für gewisse $g_{si} \in \mathbb{N}$ gilt. Wir wählen $l_{si} \in \mathbb{N}$, so dass $(l_{si} - 1)Q < g_{si} \leq l_{si} Q$. Dann definieren wir für $i = 1, \ldots, m$

$$D_i := \prod_{s=1}^{t_i} f_{si}^{l_{si}}. \tag{4}$$

Wir bemerken, dass für $i = 1, \ldots, m$ das Polynom D_i das normierte Polynom vom kleinsten Grad ist, für das $d_i \mid D_i^Q$ gilt.

Sei weiter für $k = 1, \ldots, m$: $I_k \lhd \mathcal{O}$, $c_{(k,k)} \in \mathcal{O}$ wie im Beweis von Theorem 3.2.1 definiert, insbesondere gilt $< c_{(k,k)} >= I_k$.

Lemma 3.4.2 *$D_k \in I_k$ für $k = 1, \ldots, m$.*

Beweis. Nach Konstruktion gilt $D_k \in \mathcal{O}$ für $k = 1, \ldots, m$. Für $k = 1$ müssen wir nur $D_1 w_1 \in \mathcal{O}'$ zeigen. Für $k \geq 2$ müssen wir aber nach der Definition von I_k zeigen, dass $h_1, \ldots, h_{k-1} \in \mathcal{O}$ existieren, so dass

$$\sum_{i=1}^{k-1} h_i w_i + D_k w_k \in \mathcal{O}'.$$

Es genügt jedoch zu zeigen, dass für $k = 1, \ldots, m$

$$D_k w_k \in \mathcal{O}',$$

da wir dann im Fall $k \geq 2$

$$h_1 = \ldots = h_{k-1} = 0$$

wählen können.
Sei $k \in \{1, \ldots, m\}$. Nach Konstruktion ist

$$D_k w_k \in M,$$

d.h. nach Proposition 3.3.1 genügt es, $(D_k w_k)^Q \in M$ zu beweisen. Wir betrachten also

$$D_k^Q w_k^Q = \sum_{j=1}^{m} \left(D_k^Q b_{kj} \right) w_j = \sum_{j=1}^{m} \left(D_k^Q \frac{b'_{kj}}{d_{kj}} \right) w_j.$$

Da $d_k \mid D_k^Q$ und $d_{kj} \mid d_k$ für alle $j = 1, \ldots, m$ gilt, folgt $d_{kj} \mid D_k^Q$ für $j = 1, \ldots, m$. Dann gilt

$$D_k^Q \frac{b'_{kj}}{d_{kj}} \in \mathbb{F}_q[x] = \mathcal{O},$$

und damit

$$\sum_{j=1}^{m} \left(D_k^Q \frac{b'_{kj}}{d_{kj}} \right) w_j \in M.$$

□

Folgerung 3.4.3 *Für $1 \leq k \leq m$ gilt $c_{(k,k)} \mid D_k$.*

Lemma 3.4.4 *Für jedes $k \in \{2, \ldots, m\}$ gilt: für $0 \neq a \in I_k$ existieren Elemente $a_i \in \mathcal{O}$ mit* [2]

$$deg\ a_i < deg\ c_{(i,i)}$$

für $i = 1, \ldots, k-1$, so dass

$$\sum_{i=1}^{k-1} a_i w_i + a w_k \in \mathcal{O}'.$$

Beweis. Wir fixieren ein $k \in \{2, \ldots, m\}$. Wir wählen ein $0 \neq a \in I_k$. Nach Definition von I_k existieren $\tilde{a}_i \in \mathcal{O}$, so dass

$$z := \sum_{i=1}^{k-1} \tilde{a}_i w_i + a w_k \in \mathcal{O}'.$$

Gelte $deg\ \tilde{a}_i \geq deg\ c_{(i,i)}$ für ein $i \in \{1, \ldots, k-1\}$.

Wir wählen den größten Index $j \in \{1, \ldots, k-1\}$, für den gilt:

$$deg\ \tilde{a}_j \geq deg\ c_{(j,j)}.$$

Falls $j < k-1$, folgt damit für $i = j+1, \ldots, k-1$:

$$deg\ \tilde{a}_i < deg\ c_{(i,i)}.$$

Wir setzen $a_i := \tilde{a}_i$ für $i = j+1, \ldots, k-1$.

Nach dem Euklidischen Algorithmus existieren eindeutig bestimmte Polynome $h_1, h_2 \in \mathbb{F}_q[x]$ mit $0 \leq deg\ h_2 < deg\ c_{(j,j)}$, so dass

$$\tilde{a}_j = h_1 c_{(j,j)} + h_2.$$

Damit schreiben wir z wie folgt:

$$z = \sum_{i=1}^{j-1} \tilde{a}_i w_i + \left(h_1 c_{(j,j)} + h_2\right) w_j + \sum_{i=j+1}^{k-1} a_i w_i + a w_k.$$

Nach Definition von I_j existieren $\bar{a}_i \in \mathcal{O}$ für $i = 1, \ldots, j-1$, so dass

$$\sum_{i=1}^{j-1} \bar{a}_i w_i + c_{(j,j)} w_j \in \mathcal{O}'.$$

Da $h_1 \in \mathcal{O}$, gilt

$$z - h_1 \left(\sum_{i=1}^{j-1} \bar{a}_i w_i + c_{(j,j)} w_j \right) = \sum_{i=1}^{j-1} (\tilde{a}_i - h_1 \bar{a}_i) w_i + h_2 w_j + \sum_{i=j+1}^{k-1} a_i w_i + a w_k \in \mathcal{O}'.$$

Wir setzen $a_j := h_2$. Damit gilt $deg\ a_j < deg\ c_{(j,j)}$.

Falls für ein $\bar{j} \in \{1, \ldots, j-1\}$ $deg\ (\tilde{a}_{\bar{j}} - h_1 \bar{a}_{\bar{j}}) \geq deg\ c_{(\bar{j},\bar{j})}$ gilt, führen wir das gleiche Verfahren nochmals durch. So bekommen wir nach höchstens $\bar{j}$ Schritten die gesuchten a_i für $i = 1, \ldots, k-1$.

□

[2] Für $0 = f \in \mathbb{F}_q[x]$ ist definiert: $deg\ f = -\infty$.

Lemma 3.4.5 *Für jedes $k \in \{2, \ldots, m\}$ existieren eindeutig bestimmte (bezüglich der Basis $\{w_1, \ldots, w_m\}$) Elemente $c_{(i,k)} \in \mathcal{O}$ mit*

$$deg\ c_{(i,k)} < deg\ c_{(i,i)}$$

für $i = 1, \ldots, k-1$, so dass

$$\sum_{i=1}^{k} c_{(i,k)} w_i \in \mathcal{O}'.$$

Beweis. Wir fixieren ein $k \in \{2, \ldots, m\}$. Nach Lemma 3.4.4 existieren für $c_{(k,k)} \in I_k$ Elemente $c_{(i,k)} \in \mathcal{O}$ mit $deg\ c_{(i,k)} < deg\ c_{(i,i)}$ für $i = 1, \ldots, k-1$, so dass

$$z := \sum_{i=1}^{k} c_{(i,k)} w_i \in \mathcal{O}'.$$

Existieren nun $c'_{(i,k)} \in \mathcal{O}$ mit $deg\ c'_{(i,k)} < deg\ c_{(i,i)}$ für $i = 1, \ldots, k-1$, so dass

$$c'_{(i,k)} \neq c_{(i,k)}$$

für ein $i \in \{1, \ldots, k-1\}$, und es gilt

$$z' := \sum_{i=1}^{k-1} c'_{(i,k)} w_i + c_{(k,k)} w_k \in \mathcal{O}'.$$

Damit folgt:

$$z - z' = \sum_{i=1}^{k-1} \left(c_{(i,k)} - c'_{(i,k)} \right) w_i \in \mathcal{O}'.$$

Wir wählen den größten Index $j \in \{1, \ldots, k-1\}$, für den gilt:

$$c'_{(j,k)} \neq c_{(j,k)}.$$

Damit schreiben wir $z - z'$ wie folgt:

$$z - z' = \sum_{i=1}^{j} \left(c_{(i,k)} - c'_{(i,k)} \right) w_i \in \mathcal{O}'.$$

Dann gilt: für $\left(c_{(j,k)} - c'_{(j,k)} \right) \in \mathcal{O}$ existieren Elemente $\left(c_{(i,k)} - c'_{(i,k)} \right) \in \mathcal{O}$ für $i = 1, \ldots, j-1$, so dass

$$\sum_{i=1}^{j-1} \left(c_{(i,k)} - c'_{(i,k)} \right) w_i + \left(c_{(j,k)} - c'_{(j,k)} \right) w_j \in \mathcal{O}'.$$

Nach Definition von I_j folgt

$$\left(c_{(j,k)} - c'_{(j,k)} \right) \in I_j.$$

Dann gilt

$$c_{(j,j)} \mid \left(c_{(j,k)} - c'_{(j,k)} \right).$$

Nach der Voraussetzung gilt aber

$$deg\ (c_{(j,k)} - c'_{(j,k)}) \leq max\left\{deg\ c_{(j,k)}, deg\ c'_{(j,k)}\right\} < deg\ c_{(j,j)},$$

ein Widerspruch. Damit ist $c'_{(i,k)} = c_{(i,k)}$ für $i = 1, \ldots, k-1$.

□

Sei weiter für $k = 1, \ldots, m$: $c_{(i,k)} \in \mathcal{O}$ für $i = 1, \ldots, k-1$ wie in Lemma 3.4.5 definiert.

Algorithmus 3.4.6 *Berechnung einer Ganzheitsbasis für $F'/\mathbb{F}_q(x)$.*

Seien $w_1, \ldots, w_m$ gegeben. Der Algorithmus berechnet für $k = 1, \ldots, m$ per Induktion nach k das k-te Ganzheitsbasiselement

$$u_k = \sum_{i=1}^{k} c_{(i,k)} w_i$$

mit $< c_{(k,k)} >= I_k$ und mit $c_{(i,k)} \in \mathcal{O}$ für $i = 1, \ldots, k-1$ $(k \geq 2)$.

Schritt 1. Berechnung von u_1.

Sei $k = 1$. Nach Definition von $c_{(1,1)}$ gilt

$$deg\ c_{(1,1)} = min\left\{deg\ a \mid 0 \neq a \in I_1\right\}. \tag{5}$$

Nach Proposition 3.3.1, (2) und (3) gilt:

$$c_{(1,1)} w_1 \in \mathcal{O}' \Longleftrightarrow c^Q_{(1,1)} w_1^Q \in M \Longleftrightarrow c^Q_{(1,1)} \frac{b'_{1j}}{d_{1j}} \in \mathcal{O} \text{ für } j = 1, \ldots, m \Longleftrightarrow$$

$$d_{1j} \mid c^Q_{(1,1)} \text{ für } j = 1, \ldots, m \Longleftrightarrow kgV(d_{11}, \ldots, d_{1m}) \mid c^Q_{(1,1)}. \tag{6}$$

Da $D_1 \in I_1$ (nach (4) für $i = 1$ definiert) das normierte Polynom vom kleinsten Grad ist, für das gilt

$$kgV(d_{11}, \ldots, d_{1m}) \mid D_1^Q, \tag{7}$$

folgt mit (5), (6) und (7):

$$c_{(1,1)} = D_1.$$

Damit ist $u_1 = c_{(1,1)} w_1 \in \mathcal{O}'$ bestimmt.

Schritt 2. Berechnung von u_k für ein $k \in \{2, \ldots, m\}$. Nach der Induktionsannahme für $k-1$ sind $c_{(i,i)}$ für $i = 1, \ldots, k-1$ bekannt.

Schritt 2.1. Definition einer Menge $\mathcal{M} \subseteq M$ mit $u_k \in \mathcal{M}$.

Wir setzen

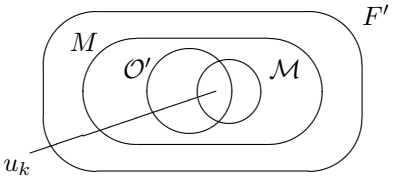
$$l_i := deg\ c_{(i,i)} - 1, \text{ für } i = 1, \ldots, k-1,$$

$$l_k := deg\ D_k.$$

Damit definieren wir die Menge $\mathcal{M} \subseteq M$ als

$$\mathcal{M} := \left\{ \sum_{i=1}^{k} a_i w_i \in F' \mid a_i \in \mathcal{O} \text{ mit } deg\ a_i \leq l_i \text{ für } i = 1, \ldots, k \right\}.$$

Nach Definition von u_k, Folgerung 3.4.3 und Lemma 3.4.5 folgt $u_k \in \mathcal{M} \cap \mathcal{O}'$.



Schritt 2.2. Beschreibung aller Elemente aus $\mathcal{M} \cap \mathcal{O}'$.

Wir setzen

$$l_0 := 0,$$
$$l := \sum_{i=1}^{k} (l_i + 1)$$

und definieren die folgende Funktion für $i = 1, \ldots, k$ und für $s = 0, \ldots, l_i$

$$\phi(i, s) := \sum_{j=0}^{i-1} (l_j + 1) + s.$$

Der Wertebereich von ϕ ist gleich $\{1, \ldots, l\}$. Damit können wir eine Bijektion zwischen $\mathbb{F}_q^l$ und $\mathcal{M}$ wie folgt definieren:
1. Jedes $e = (e_1^*, \ldots, e_l^*) \in \mathbb{F}_q^l$ definiert für $i = 1, \ldots, k$ Polynome

$$a_i := \sum_{s=0}^{l_i} e^*_{\phi(i,s)} x^s \in \mathbb{F}_q[x],$$

so dass

$$z_e := \sum_{i=1}^{k} a_i w_i \in \mathcal{M}.$$

2. Für jedes $z \in \mathcal{M}$ mit der Darstellung

$$z = \sum_{i=1}^{k} a_i w_i,$$

wobei

$$a_i = \sum_{s=0}^{l_i} e^{\times}_{is} x^s \in \mathbb{F}_q[x]$$

mit $e^{\times}_{is} \in \mathbb{F}_q$ für $i = 1, \ldots, k$ und für $s = 0, \ldots, deg\ a_i$, und $e^{\times}_{is} := 0$ für $s > deg\ a_i$, existiert genau ein

$$e_z = (e_1^*, \ldots, e_l^*) \in \mathbb{F}_q^l,$$

so dass

$$e^*_{\phi(i,s)} = e^{\times}_{is} \text{ für } i = 1, \ldots, k \text{ und für } s = 0, \ldots, l_i.$$

Wir definieren einen Unterraum $E \subseteq \mathbb{F}_q^l$ wie folgt:

$$E := \left\{ e \in \mathbb{F}_q^l \mid z_e \in \mathcal{M} \cap \mathcal{O}' \right\}.$$

Sei $d := dim_{\mathbb{F}_q} E$ und $\{v_1, \ldots, v_d\}$ eine Basis von E. Dann existiert für jedes $z \in \mathcal{M} \cap \mathcal{O}'$ genau eine Folge $\lambda_1^*, \ldots, \lambda_d^* \in \mathbb{F}_q$, so dass

$$e_z = \sum_{t=1}^{d} \lambda_t^* v_t.$$

Daher folgt: **finden wir eine Basis von E, beschreiben wir damit die Menge $\mathcal{M} \cap \mathcal{O}'$.**

Wir starten mit einem Tupel von Unbestimmten $(e_1, \ldots, e_l)$ und setzen

$$\begin{aligned} a_i(e_1, \ldots, e_l, x) &:= \sum_{s=0}^{l_i} e_{\phi(i,s)} x^s \quad \text{für } i = 1, \ldots, k, \\ z(e_1, \ldots, e_l) &:= \sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x) w_i. \end{aligned} \tag{8}$$

Nach Proposition 3.3.1 gilt für jedes $z \in \mathcal{M}$:

$$z \in \mathcal{O}' \Longleftrightarrow z \in M \text{ und } z^Q \in M.$$

Daher betrachten wir $z(e_1, \ldots, e_l)^Q$:

$$\begin{aligned} z(e_1, \ldots, e_l)^Q &= \left(\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x) w_i \right)^Q \\ &= \left(\sum_{i=1}^{k} \left(\sum_{s=0}^{l_i} e_{\phi(i,s)} x^s \right) w_i \right)^Q. \end{aligned}$$

Wir bemerken, dass wir ein $n_1 \in \mathbb{N}$ so wählen können, dass $Q \leq q^{n_1}$ ist. Damit erfüllt auch q^{n_1} den Punkt (4) im Abschnitt 3.1, und es gilt demnach das Ganzheitskriterium aus Proposition 3.3.1: $z \in \mathcal{O}' \Longleftrightarrow z \in M$ und $z^{q^{n_1}} \in M$. Daher wählen wir für folgende Berechnungen o.E.

$$Q = q^{n_1}.$$

Da $Char\ F' = p$, folgt:

$$z(e_1, \ldots, e_l)^Q = \sum_{i=1}^{k} \left(\sum_{s=0}^{l_i} {e_{\phi(i,s)}}^Q x^{sQ} \right) w_i^Q.$$

Nach (2) (Seite 16) gilt:

$$\begin{aligned} z(e_1, \ldots, e_l)^Q &= \sum_{i=1}^{k} \left(\sum_{s=0}^{l_i} {e_{\phi(i,s)}}^Q x^{sQ} \right) \sum_{j=1}^{m} b_{ij} w_j \\ &= \sum_{j=1}^{m} \left(\sum_{i=1}^{k} \sum_{s=0}^{l_i} {e_{\phi(i,s)}}^Q x^{sQ} b_{ij} \right) w_j. \end{aligned}$$

Da es vorausgesetzt ist, dass $e_1, \ldots, e_l$ ihre Werte aus $\mathbb{F}_q$ annehmen werden, folgt ${e_i}^Q = e_i$ für $i = 1, \ldots, l$. Damit gilt:

$$\begin{aligned} z(e_1, \ldots, e_l)^Q &= \sum_{j=1}^{m} \left(\sum_{i=1}^{k} \sum_{s=0}^{l_i} e_{\phi(i,s)} x^{sQ} b_{ij} \right) w_j \\ &= \sum_{j=1}^{m} \left(\frac{\sum_{i=1}^{k} \sum_{s=0}^{l_i} e_{\phi(i,s)} x^{sQ} b''_{ij}}{kgV(d_{1j}, \ldots, d_{kj})} \right) w_j, \end{aligned} \tag{9}$$

wobei $b''_{ij} := b_{ij} \cdot kgV(d_{1j}, \ldots, d_{kj}) \in \mathbb{F}_q[x]$ mit b_{ij} für $i, j = 1, \ldots, m$ wie in (3) (Seite 16) definiert.

Sind $e_i = e_i^* \in \mathbb{F}_q$ für $i = 1, \ldots, l$ und gilt $(e_1^*, \ldots, e_l^*) \in E$, folgt

$$z(e_1^*, \ldots, e_l^*) \in \mathcal{O}' \Longleftrightarrow z(e_1^*, \ldots, e_l^*)^Q \in M \Longleftrightarrow$$

$$\left(\frac{\sum_{i=1}^{k} \sum_{s=0}^{l_i} e^*_{\phi(i,s)} x^{sQ} b''_{ij}}{kgV(d_{1j}, \ldots, d_{kj})} \right) \in \mathbb{F}_q[x] \text{ für } j = 1, \ldots, m.$$

Daher müssen wir feststellen, unter welchen Voraussetzungen für $j = 1, \ldots, m$ gilt:

$$\left(\frac{\sum_{i=1}^{k} \sum_{s=0}^{l_i} e_{\phi(i,s)} x^{sQ} b''_{ij}}{kgV(d_{1j}, \ldots, d_{kj})} \right) \in \mathbb{F}_q(e_1, \ldots, e_l)[x].^3 \tag{10}$$

Wir setzen für $j = 1, \ldots, m$:

$$\begin{aligned} Z_j &:= \sum_{i=1}^{k} \sum_{s=0}^{l_i} e_{\phi(i,s)} x^{sQ} b''_{ij} \in \mathbb{F}_q(e_1, \ldots, e_l)[x], \\ N_j &:= kgV(d_{1j}, \ldots, d_{kj}) \in \mathbb{F}_q[x]. \end{aligned}$$

Da $\mathbb{F}_q[x] \subset \mathbb{F}_q(e_1, \ldots, e_l)[x]$ und $deg\ Z_j \geq deg\ N_j$,[4] existieren nach dem Euklidischen Algorithmus Polynome $Q_j, R_j \in \mathbb{F}_q(e_1, \ldots, e_l)[x]$, so dass gilt: $Z_j = Q_j N_j + R_j$ und $deg\ R_j < deg\ N_j$. Ist $R_j = 0$ für $j = 1, \ldots, m$, folgt (10). Daher werden wir die Division von Z_j durch N_j für $j = 1, \ldots, m$ durchführen und dabei zeigen, dass die Bedingungen $R_j = 0$ für $j = 1, \ldots, m$ auf ein lineares Gleichungssystem über $\mathbb{F}_q$ mit den Unbestimmten $e_1, \ldots, e_l$ hinauslaufen.

Sei $j \in \{1, \ldots, m\}$. Wir bezeichnen die Menge aller $\mathbb{F}_q$-linearen Ausdrücke in den Unbestimmten $e_1, \ldots, e_l$ mit

$$\bar{E} := \left\{ \sum_{i=1}^{l} \gamma_i e_i \mid \gamma_i \in \mathbb{F}_q, \text{ für } i = 1, \ldots, l \right\}.$$

Sei $h_j^{(0)} := max\{Q \cdot l_i + deg\ b''_{ij} \mid i = 1, \ldots, k\}$. Dann gilt:

$$Z_j = \sum_{t=0}^{h_j^{(0)}} \alpha_{jt}^{(0)} x^t$$

für gewisse $\alpha_{jt}^{(0)} \in \bar{E}$ für $t = 0, \ldots, h_j^{(0)}$.

[3] $\mathbb{F}_q(e_1, \ldots, e_l)$ ist der Körper der rationalen Funktionen in den Unbestimmten $e_1, \ldots, e_l$.
[4] Gilt wegen $\{0\} \subsetneqq \mathcal{M} \cap \mathcal{O}'$.

Sei $s_j^{(0)} := h_j^{(0)} - deg\ N_j$. Dann definieren wir

$$Z_j^{(1)} := Z_j - \alpha_{jh_j^{(0)}}^{(0)} x^{s_j^{(0)}} N_j,$$

und es gilt

$$Z_j^{(1)} := \sum_{t=0}^{h_j^{(1)}} \alpha_{jt}^{(1)} x^t$$

für ein $h_j^{(1)} < h_j^{(0)}$ (N_j ist normiert), für ein $\alpha_{jh_j^{(1)}}^{(1)} \neq 0$ und für gewisse $\alpha_{jt}^{(1)} \in \bar{E}$ für $t = 0, \ldots, h_j^{(1)}$.

Ist $h_j^{(1)} \geq deg\ N_j$, sei $s_j^{(1)} := h_j^{(1)} - deg(N_j)$. Dann definieren wir

$$Z_j^{(2)} := Z_j^{(1)} - \alpha_{jh_j^{(1)}}^{(1)} x^{s_j^{(1)}} N_j,$$

und es gilt

$$Z_j^{(2)} := \sum_{t=0}^{h_j^{(2)}} \alpha_{jt}^{(2)} x^t$$

für ein $h_j^{(2)} < h_j^{(1)}$ (N_j ist normiert), für ein $\alpha_{jh_j^{(2)}}^{(2)} \neq 0$ und für gewisse $\alpha_{jt}^{(2)} \in \bar{E}$ für $t = 0, \ldots, h_j^{(2)}$.

Ist wieder $h_j^{(2)} \geq deg\ N_j$, so fahren wir analog weiter fort. Dann existiert ein $r_j \leq h_j^{(0)} - deg\ N_j + 1$, so dass gilt:

$$Z_j = N_j \sum_{t=0}^{r_j - 1} \alpha_{jh_j^{(t)}}^{(t)} x^{s_j^{(t)}} + \sum_{t=0}^{h_j^{(r_j)}} \alpha_{jt}^{(r_j)} x^t$$

mit $h_j^{(r_j)} < deg\ N_j$ und für gewisse $\alpha_{jt}^{(r_j)} \in \bar{E}$ für $t = 0, \ldots, h_j^{(r_j)}$ und $\alpha_{jh_j^{(r_j)}}^{(r_j)} \neq 0$.

Wir setzen

$$R_j := \sum_{t=0}^{h_j^{(r_j)}} \alpha_{jt}^{(r_j)} x^t.$$

Dann gilt:

$$(10) \text{ ist erfüllt} \iff R_j = 0 \text{ für } j = 1, \ldots, m. \tag{11}$$

Da $\alpha_{jt}^{(r_j)} \in \bar{E}$ für $j = 1, \ldots, m$ und für $t = 0, \ldots, h_j^{(r_j)}$, gilt

$$\alpha_{jt}^{(r_j)} = \sum_{i=1}^{l} \gamma_{jti} e_i$$

für gewisse $\gamma_{jti} \in \mathbb{F}_q$ für $j = 1, \ldots, m$, für $t = 0, \ldots, h_j^{(r_j)}$ und für $i = 1, \ldots, l$. Nach (11) folgt

$$(10) \text{ ist erfüllt} \iff \sum_{i=1}^{l} \gamma_{jti} e_i = 0 \text{ für } j = 1, \ldots, m \text{ und für } t = 0, \ldots h_j^{(r_j)}.$$

Wir betrachten diese Bedingungen als Gleichungen über $\mathbb{F}_q$ mit den Unbestimmten $e_1, \ldots, e_l$:

$$\begin{aligned}
&\sum_{i=1}^{l} \gamma_{10i} e_i = 0 \\
&\qquad \vdots \\
&\sum_{i=1}^{l} \gamma_{1h_1^{(r_1)}i} e_i = 0 \\
&\qquad \vdots \\
&\sum_{i=1}^{l} \gamma_{m0i} e_i = 0 \\
&\qquad \vdots \\
&\sum_{i=1}^{l} \gamma_{mh_m^{(r_m)}i} e_i = 0
\end{aligned} \tag{12}$$

Zusammen bilden diese Gleichungen ein homogenes lineares Gleichungssystem über $\mathbb{F}_q$ mit den Unbestimmten $e_1, \ldots, e_l$. Hat das Gleichungssystem nur die triviale Lösung, so folgt $E = \{(0, \ldots, 0)\}$, und damit gilt $\mathcal{M} \cap \mathcal{O}' = \{0\}$, was $0 \neq u_k \in \mathcal{M} \cap \mathcal{O}'$ widerspricht. Daher besitzt das System mehrere Lösungen.

Mit dem Gaußschen Algorithmus können wir eine $\mathbb{F}_q$-Basis $\{v_1, \ldots, v_d\}$ von E bestimmen, wobei $v_t = (v_{1t}, \ldots, v_{lt})$ für $t = 1, \ldots, d$ sind. Dann ist der Vektorraum E gleich

$$E = \left\{ (e_1, \ldots, e_l) \in \mathbb{F}_q^l \;\middle|\; \begin{array}{l} \text{es existieren } \lambda_1^*, \ldots, \lambda_d^* \in \mathbb{F}_q, \text{ so dass} \\ e_i = \sum_{t=1}^{d} \lambda_t^* v_{it} \text{ für } i = 1, \ldots, l \end{array} \right\},$$

und wir können die Menge $\mathcal{M} \cap \mathcal{O}'$ wie folgt beschreiben:

$$\mathcal{M} \cap \mathcal{O}' = \left\{ z \in F' \;\middle|\; \begin{array}{l} \text{es existiert ein } (e_1^*, \ldots, e_l^*) \in E, \text{ so} \\ \text{dass } z = \sum_{i=1}^{k} \left(\sum_{s=0}^{l_i} e^*_{\phi(i,s)} x^s \right) w_i \end{array} \right\}. \tag{13}$$

Schritt 2.3. Berechnung von $c_{(k,k)} \in \mathbb{F}_q[x]$ mit $< c_{(k,k)} >= I_k$.

Sei $\mathbb{F}_q(\lambda_1, \ldots, \lambda_d)$ der Körper der rationalen Funktionen in den Unbestimmten $\lambda_1, \ldots, \lambda_d$. Dann definieren wir für $i = 1, \ldots, k$

$$a_i(\lambda_1, \ldots, \lambda_d, x) := \sum_{s=0}^{l_i} \left(\sum_{t=1}^{d} \lambda_t v_{\phi(i,s)t} \right) x^s \in \mathbb{F}_q(\lambda_1, \ldots, \lambda_d)[x]. \tag{14}$$

Seien $\lambda_1^*, \ldots, \lambda_d^* \in \mathbb{F}_q$ und $\lambda_t = \lambda_t^*$ für $t = 1, \ldots, d$. Dann gilt nach (14) $a_i(\lambda_1^*, \ldots, \lambda_d^*, x) \in \mathbb{F}_q[x]$, und nach (13) und Definition von I_k (Theorem 3.2.1) für $k = 1, \ldots, m$

$$a_k(\lambda_1^*, \ldots, \lambda_d^*, x) \in I_k. \tag{15}$$

BEHAUPTUNG. Es gilt

$$c_{(k,k)} \mid a_k(\lambda_1, \ldots, \lambda_d, x), ^5$$

[5] Die Teilbarkeit wird hier in $\mathbb{F}_q(\lambda_1, \ldots, \lambda_d)[x]$ betrachtet.

wobei $c_{(k,k)}$ das normierte Polynom vom größten Grad aus $\mathbb{F}_q[x]$ mit dieser Eigenschaft ist.

BEWEIS. Da $deg\ a_k(\lambda_1,\ldots,\lambda_d,x) \geq deg\ c_{(k,k)}$ gilt, kann die Division von $a_k(\lambda_1,\ldots,\lambda_d,x)$ durch $c_{(k,k)}$ durchgeführt werden. Sei der Rest dieser Division ungleich 0. Dann folgt analog zur Division[6] in (10), dass dieser Rest ein Polynom in $\mathbb{F}_q(\lambda_1,\ldots,\lambda_d)[x]$ ist, dessen Koeffizienten lineare Ausdrücke über $\mathbb{F}_q$ in den Unbestimmten $\lambda_1,\ldots,\lambda_d$ sind. Wir bezeichnen daher diesen Rest mit $r(\lambda_1,\ldots,\lambda_d,x)$. Dann existieren $\lambda_1^*,\ldots,\lambda_d^* \in \mathbb{F}_q$, so dass bei $\lambda_t = \lambda_t^*$ für $t = 1,\ldots,d$ gilt: $r(\lambda_1^*,\ldots,\lambda_d^*,x) \neq 0$. Damit folgt $c_{(k,k)} \nmid a_k(\lambda_1^*,\ldots,\lambda_d^*,x)$, was ein Widerspruch zu (15) ist.

Existiert ein normiertes Polynom $h \in \mathbb{F}_q[x]$ mit $deg\ h > deg\ c_{(k,k)}$ und gilt dabei $h \mid a_k(\lambda_1,\ldots,\lambda_d,x)$, so folgt bei jeder Wahl $\lambda_t = \lambda_t^* \in \mathbb{F}_q$ für $t = 1,\ldots,d$: $h \mid a_k(\lambda_1^*,\ldots,\lambda_d^*,x)$. Da aber durch $a_k(\lambda_1,\ldots,\lambda_d,x)$ alle Polynome mit den Graden kleiner oder gleich $l_k = deg\ D_k$ aus $I_k \lhd \mathbb{F}_q[x]$ beschrieben sind, folgt ein Widerspruch zu $< c_{(k,k)} > = I_k$. $\lhd$

Daher kann das Polynom $c_{(k,k)}$ wie folgt berechnet werden:

$$c_{(k,k)} = ggT_{\mathbb{F}_q(\lambda_1,\ldots,\lambda_d)[x]}(a_k(\lambda_1,\ldots,\lambda_d,x), D_k). \tag{16}$$

Schritt 2.4. Berechnung von $c_{(i,k)} \in \mathbb{F}_q[x]$ für $i = 1,\ldots,k-1$.

Da $c_{(i,k)}$ für $i = 1,\ldots,k-1$ nach Lemma 3.4.5 eindeutig bestimmt sind, existieren eindeutig bestimmte $\lambda_1^\times,\ldots,\lambda_d^\times \in \mathbb{F}_q$, so dass

$$c_{(i,k)} = a_i(\lambda_1^\times,\ldots,\lambda_d^\times,x)$$

für $i = 1,\ldots,k$. So müssen wir diese $\lambda_1^\times,\ldots,\lambda_d^\times \in \mathbb{F}_q$ finden.

Wir schreiben $c_{(k,k)}$ als

$$c_{(k,k)} = \sum_{s=0}^{deg\ c_{(k,k)}} \gamma_{ks} x^s$$

für gewisse $\gamma_{ks} \in \mathbb{F}_q$ für $s = 0,\ldots,deg\ c_{(k,k)}$. Wir setzen koeffizientenweise nach (14) für $i = k$:

$$a_k(\lambda_1,\ldots,\lambda_d,x) = c_{(k,k)},^7$$

d.h.

$$\sum_{t=1}^{d} \lambda_t v_{\phi(k,s)t} = \gamma_{ks} \qquad \text{für } s = 0,\ldots,deg\ c_{(k,k)},$$

$$\sum_{t=1}^{d} \lambda_t v_{\phi(k,s)t} = 0 \qquad \text{für } s = deg\ c_{(k,k)}+1,\ldots,l_k.$$

Die obigen Gleichungen bilden ein lineares Gleichungssystem über $\mathbb{F}_q$ mit den Unbestimmten $\lambda_1,\ldots,\lambda_d$. Wegen der Eindeutigkeit von $c_{(k,k)}$ hat dieses System genau eine Lösung

$$(\lambda_1^\times,\ldots,\lambda_d^\times) \in \mathbb{F}_q^d.$$

[6] Diese Division ist ausführlich auf den Seiten 23 - 24 beschrieben.

[7] Würden nicht alle Unbestimmten $\lambda_1,\ldots,\lambda_d$ in $a_k(\lambda_1,\ldots,\lambda_d,x)$ in (14) vorkommen, wären die zu $c_{(k,k)}$ zugehörigen $c_{(i,k)}$ wegen der nichtvorkommenden Unbestimmten nicht eindeutig bestimmt, was Lemma 3.4.5 widersprechen würde.

Mit dieser Lösung erhalten wir für $i = 1, \ldots, k-1$

$$c_{(i,k)} = a_i(\lambda_1^\times, \ldots, \lambda_d^\times, x). \tag{17}$$

Damit ist durch (16) und (17)

$$u_k = \sum_{i=1}^{k} c_{(i,k)} w_i \in \mathcal{O}' \tag{18}$$

bestimmt.

Nach Theorem 3.2.1 bilden $u_1, \ldots, u_m$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$.

□

Theorem 3.4.7 *Mit dem Algorithmus 3.4.6 ist eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ explizit berechenbar.*

Theorem 3.4.7 garantiert uns nicht, dass die mittels Algorithmus 3.4.6 berechnete Ganzheitsbasis $\{u_1, \ldots, u_m\}$ für $F'/\mathbb{F}_q(x)$ aus Elementen mit modulo m paarweise inkongruenten Polordnungen an der Stelle P'_∞ besteht, was für die Berechnung von Basen für die Vektorräume $\mathcal{L}(rP'_\infty)$ erforderlich ist. Daher werden wir im nächsten Abschnitt noch einen Algorithmus angeben, mittels dessen wir eine solche Ganzheitsbasis berechnen können.

3.5 Ganzheitsbasen für $F'/\mathbb{F}_q(x)$ mit modulo m paarweise inkongruenten Polordnungen an der Stelle P'_∞

Nach Definition 2.1.20 und Theorem 2.1.21 können wir folgende Vorbereitungen durchführen.

Wir setzen für $i = 1, \ldots, m$

$$\nu_i := min\{\alpha \in \mathbb{N} \cup \{0\} \mid \alpha \text{ ist eine Polzahl von } P'_\infty \text{ mit } \alpha \equiv i \ mod \ m\}.$$

Seien $y_1, \ldots, y_m \in \mathcal{O}'$, so dass

$$v_{P'_\infty}(y_i) = -\mu_i$$

mit

$$\mu_i \in \mathbb{N} \cup \{0\} \text{ und } \mu_i \equiv i \ mod \ m$$

für $i = 1, \ldots, m$ gilt.

Lemma 3.5.1 *1. $\{y_1, \ldots, y_m\}$ ist eine Basis für $F'/\mathbb{F}_q(x)$.*
2. α ist eine Polzahl von P'_∞ dann und nur dann, wenn ein $z \in \mathcal{O}'$ existiert mit $v_{P'_\infty}(z) = -\alpha$.
3. Seien $z_1, z_2 \in \mathcal{O}'$ mit $v_{P'_\infty}(z_1) = v_{P'_\infty}(z_2)$. Dann existiert genau ein $a \in \mathbb{F}_q^*$, so dass $v_{P'_\infty}(z_1 - az_2) > v_{P'_\infty}(z_1)$.

Beweis. 1. Da $[F' : \mathbb{F}_q(x)] = m$, genügt es zu zeigen, dass $y_1, \ldots, y_m$ linear unabhängig über $\mathbb{F}_q(x)$ sind. Dies folgt nach Lemma 2.1.8.
2. Dies gilt wegen $\mathcal{O}' = \bigcup_{s \geq 0}^{\infty} \mathcal{L}(sP'_\infty)$.
3. Wegen $v_{P'_\infty}\left(\frac{z_1}{z_2}\right) = 0$ und $deg\ P'_\infty = 1$ existiert ein $a \in \mathbb{F}_q^*$, so dass $v_{P'_\infty}\left(\frac{z_1}{z_2} - a\right) > 0$.

□

Theorem 3.5.2 *$\{y_1, \ldots, y_m\}$ ist eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ dann und nur dann, wenn $\mu_i = \nu_i$ für $i = 1, \ldots, m$.*

Beweis. $\Longrightarrow$ Sei $\{y_1, \ldots, y_m\}$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$. Sei $j \in \{1, \ldots, m\}$. Dann ist nach Lemma 3.5.1(2) μ_j eine Polzahl von P'_∞, und es gilt:

$$\mu_j \geq \nu_j. \tag{19}$$

Da ν_j eine Polzahl von P'_∞ ist, existiert nach Lemma 3.5.1(2) ein $z \in \mathcal{O}'$ mit $v_{P'_\infty}(z) = -\nu_j$. Da $z \in \mathcal{O}'$, hat es die Gestalt

$$z = \sum_{i=1}^{m} f_i y_i$$

mit $f_i \in \mathcal{O} = \mathbb{F}_q[x]$. Dann gilt wegen $\nu_j \equiv \mu_j \ mod\ m$:

$$v_{P'_\infty}(z) = v_{P'_\infty}(f_j y_j).$$

Daraus folgt $-\nu_j = -m \cdot deg\ f_j - \mu_j$. Damit gilt

$$\nu_j \geq \mu_j. \tag{20}$$

Aus (19) und (20) folgt $\nu_j = \mu_j$.

$\Longleftarrow$ Sei $\mu_i = \nu_i$ für $i = 1, \ldots, m$. Nach Lemma 3.5.1(1) bilden $y_1, \ldots, y_m \in \mathcal{O}'$ eine Basis für $F'/\mathbb{F}_q(x)$, und es gilt $\sum_{i=1}^{m} \mathcal{O} y_i \subseteq \mathcal{O}'$. Wir zeigen, dass auch $\mathcal{O}' \subseteq \sum_{i=1}^{m} \mathcal{O} y_i$ gilt.

Wir wählen ein $0 \neq z \in \mathcal{O}'$ mit $(z)_\infty^{F'} = sP'_\infty$ für ein $s \in \mathbb{N} \cup \{0\}$. Wir zeigen die Inklusion $\mathcal{O}' \subseteq \sum_{i=1}^{m} \mathcal{O} y_i$ per Induktion nach s.

Sei $s = 0$. Dann gilt $z \in \mathbb{F}_q^*$. Da 0 eine Polzahl von P'_∞ ist, folgt $\nu_m = 0$. Damit ist $(y_m)_\infty^{F'} = 0$, und $y_m \in \mathbb{F}_q^*$. Dann gilt:

$$z \in \mathbb{F}_q^* \subseteq \mathcal{O} y_m \subseteq \sum_{i=1}^{m} \mathcal{O} y_i.$$

Wir zeigen den Schritt $s \to s+1$. Dann gilt $(z)_\infty^{F'} = (s+1)P'_\infty$. Sei $j \in \{1, \ldots, m\}$, so dass $s+1 \equiv j \ mod\ m$. Dann gilt:

$$\begin{aligned}
\nu_j \equiv s+1 \ mod\ m \text{ und } \nu_j \leq s+1 \quad &\Longrightarrow \quad s+1 = \nu_j + m \cdot t \text{ für ein } t \in \mathbb{N} \cup \{0\} \\
&\Longrightarrow \quad v_{P'_\infty}(z) = v_{P'_\infty}\left(y_j x^t\right) \\
&\Longrightarrow \quad \text{nach Lemma 3.5.1(3) existiert genau} \\
&\qquad\quad \text{ein } a \in \mathbb{F}_q^*, \text{ so dass} \\
&\qquad\quad v_{P'_\infty}\left(z - a x^t y_j\right) > -(s+1).
\end{aligned}$$

Das Element $z - a x^t y_j$ liegt in $\mathcal{O}'$, und seine Polordnung an der Stelle P'_∞ ist kleiner als $s+1$. Nach Induktionsannahme gilt $z - a x^t y_j \in \sum_{i=1}^{m} \mathcal{O} y_i$. Daher ist $z \in \sum_{i=1}^{m} \mathcal{O} y_i$.

□

Nun wissen wir nach Theorem 3.5.2, dass eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ existiert, die aus Elementen mit modulo m paarweise inkongruenten Polordnungen an der Stelle P'_∞ besteht. Der folgende Algorithmus berechnet aus einer

Ganzheitsbasis für $F'/\mathbb{F}_q(x)$, die mittels Algorithmus 3.4.6 erhalten wurde, eine weitere Ganzheitsbasis, deren Elemente modulo m paarweise inkongruente Polordnungen an der Stelle P'_∞ haben.

Algorithmus 3.5.3 *Berechnung einer Ganzheitsbasis $\{u_1^*, \ldots, u_m^*\}$ für $F'/\mathbb{F}_q(x)$ mit $v_{P'_\infty}(u_i^*) \not\equiv v_{P'_\infty}(u_j^*)$ mod m für $i, j = 1, \ldots, m$ und $i \neq j$ unter folgenden Voraussetzungen:*
(1) die Basis $\{w_1, \ldots, w_m\}$ für $F'/\mathbb{F}_q(x)$ aus Abschnitt 3.1(2) ist bekannt, und eine Ganzheitsbasis $\{u_1, \ldots, u_m\}$ für $F'/\mathbb{F}_q(x)$ ist mittels Algorithmus 3.4.6 berechnet worden;
(2) $v_{P'_\infty}(w_i) \not\equiv v_{P'_\infty}(w_j)$ mod m für $i, j = 1, \ldots, m$ und $i \neq j$.

Die zweite Bedingung ist für die Berechnung von $v_{P'_\infty}(u_k)$ (Lemma 2.1.8) für $k = 1, \ldots, m$ erforderlich: wir setzen $c_{(i,k)} := 0$ für $k = 1, \ldots, m$ und für $i = k+1, \ldots, m$, damit hat u_k aus (18) ab jetzt die Darstellung

$$u_k = \sum_{i=1}^{m} c_{(i,k)} w_i, \tag{21}$$

und es gilt

$$\begin{aligned} v_{P'_\infty}(u_k) &= v_{P'_\infty}\left(\sum_{i=1}^{m} c_{(i,k)} w_i\right) \\ &= min_{i=1,\ldots,m}\left\{v_{P'_\infty}\left(c_{(i,k)} w_i\right)\right\} \\ &= -m \cdot deg\ c_{(i',k)} + v_{P'_\infty}(w_{i'}) \quad \text{für ein } i' \in \{1, \ldots, m\}. \end{aligned} \tag{22}$$

Die Darstellung (21) ist für den Ablauf des Algorithmus erforderlich.

Schritt 1. Fixierung von $k_1 \neq k_2$, für die $v_{P'_\infty}(u_{k_1}) \equiv v_{P'_\infty}(u_{k_2})$ mod m gilt. Werden keine solchen Indizes gefunden, so ist der Algorithmus beendet. Die vorhandenen Ganzheitsbasiselemente haben bereits modulo m paarweise inkongruente Polordnungen an der Stelle P'_∞.

So haben wir:

$$u_{k_1} = \sum_{i=1}^{m} c_{(i,k_1)} w_i \text{ und } u_{k_2} = \sum_{i=1}^{m} c_{(i,k_2)} w_i$$

mit

$$v_{P'_\infty}(u_{k_1}) \equiv v_{P'_\infty}(u_{k_2}) \ mod\ m.$$

Schritt 2. Fixierung von $s \in \{1, \ldots, m\}$ mit $v_{P'_\infty}(u_{k_1}) \equiv v_{P'_\infty}(w_s)$ mod m.

Wegen (22) folgt:

$$\begin{aligned} v_{P'_\infty}(u_{k_1}) &= v_{P'_\infty}\left(c_{(s,k_1)} w_s\right) = -m \cdot deg\ c_{(s,k_1)} + v_{P'_\infty}(w_s), \\ v_{P'_\infty}(u_{k_2}) &= v_{P'_\infty}\left(c_{(s,k_2)} w_s\right) = -m \cdot deg\ c_{(s,k_2)} + v_{P'_\infty}(w_s). \end{aligned}$$

Ohne Einschränkung können wir annehmen, dass

$$v_{P'_\infty}(u_{k_1}) \leq v_{P'_\infty}(u_{k_2}). \tag{23}$$

Schritt 3. Berechnung eines neuen Elements $\tilde{u} \in \mathcal{O}'$, für das $v_{P'_\infty}(\tilde{u}) > v_{P'_\infty}(u_{k_1})$ gilt, und Ersetzung von u_{k_1} durch $\tilde{u}$, so dass Elemente $u_1, \ldots, \tilde{u}($ an der Stelle von $u_{k_1}), \ldots, u_m$ eine weitere Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ bilden.

Wegen (23) folgt $deg\ c_{(s,k_1)} \geq deg\ c_{(s,k_2)}$. Dann gilt für ein $t \in \mathbb{N} \cup \{0\}$:

$$deg\ c_{(s,k_1)} = deg\ (x^t c_{(s,k_2)}) \Longrightarrow v_{P'_\infty}(u_{k_1}) = v_{P'_\infty}(x^t u_{k_2}).$$

Sei $\gamma \in \mathbb{F}_q^*$, so dass

$$\gamma = \frac{\text{Leitkoeffizient des Polynoms } c_{(s,k_1)}}{\text{Leitkoeffizient des Polynoms } c_{(s,k_2)}}.$$

Sei

$$\tilde{u} := u_{k_1} - \gamma x^t u_{k_2}.$$

BEHAUPTUNG. $v_{P'_\infty}(\tilde{u}) > v_{P'_\infty}(u_{k_1})$.
BEWEIS. Wegen $v_{P'_\infty}(w_i) \not\equiv v_{P'_\infty}(w_j)\ mod\ m$ für $i, j = 1, \ldots, m$ und $i \neq j$ folgt

$$\begin{aligned} v_{P'_\infty}(\tilde{u}) &= min_{i=1,\ldots,m} \left\{ v_{P'_\infty} \left(\left(c_{(i,k_1)} - \gamma x^t c_{(i,k_2)} \right) w_i \right) \right\} \\ &= v_{P'_\infty} \left(\left(c_{(v,k_1)} - \gamma x^t c_{(v,k_2)} \right) w_v \right) \qquad \text{für ein gewisses } v \in \{1, \ldots, m\}. \end{aligned}$$

Falls $v \neq s$, gilt nach (22) für alle $i = 1, \ldots, m$ und $i \neq s$ (insbesondere für $i = v$)

$$v_{P'_\infty}(u_{k_1}) = v_{P'_\infty} \left(c_{(s,k_1)} w_s \right) = v_{P'_\infty} \left(\gamma x^t c_{(s,k_2)} w_s \right) < v_{P'_\infty} \left(\gamma x^t c_{(i,k_2)} w_i \right)$$

und

$$v_{P'_\infty}(u_{k_1}) = v_{P'_\infty} \left(c_{(s,k_1)} w_s \right) < v_{P'_\infty} \left(c_{(i,k_1)} w_i \right).$$

Damit folgt

$$v_{P'_\infty}(\tilde{u}) \geq min \left\{ v_{P'_\infty} \left(c_{(v,k_1)} w_v \right), v_{P'_\infty} \left(\gamma x^t c_{(v,k_2)} w_v \right) \right\} > v_{P'_\infty}(u_{k_1}).$$

Falls $v = s$, folgt wegen der Wahl von γ

$$deg\ (c_{(s,k_1)} - \gamma x^t c_{(s,k_2)}) < deg\ c_{(s,k_1)}, \tag{24}$$

und damit gilt

$$v_{P'_\infty}(\tilde{u}) = v_{P'_\infty} \left(\left(c_{(s,k_1)} - \gamma x^t c_{(s,k_2)} \right) w_s \right) > v_{P'_\infty} \left(c_{(s,k_1)} w_s \right) = v_{P'_\infty}(u_{k_1}).$$

Da nach Lemma 3.5.1(3) genau ein $a \in \mathbb{F}_q^*$ existiert, so dass

$$v_{P'_\infty} \left(u_{k_1} - a x^t u_{k_2} \right) > v_{P'_\infty}(u_{k_1})$$

gilt, folgt $v_{P'_\infty}(\tilde{u}) > v_{P'_\infty}(u_{k_1})$ nur für diese Wahl von γ. $\lhd$

Da $\{u_1, \ldots, u_m\}$ eine Basis für $\mathcal{O}'/\mathbb{F}_q[x]$ ist, folgt

$$\begin{aligned} \sum_{i=1}^{m} h_i(x) u_i = 0 \quad &\Longleftrightarrow \quad 0 = h_i(x) \in \mathbb{F}_q[x] \text{ für } i = 1, \ldots, m \\ &\Longleftrightarrow \quad \sum_{\substack{i \in \{1, \ldots, m\} \\ i \neq k_1}} h_i(x) u_i + h_{k_1}(x) \left(\tilde{u} + \gamma x^t u_{k2} \right) = 0. \end{aligned}$$

Damit sind die Elemente der Menge $\{u_1, \ldots, u_m\} \cup \{\tilde{u}\} \setminus \{u_{k_1}\}$ linear unabhängig über $\mathbb{F}_q[x]$. Aus $\mathcal{O}' = \sum_{i=1}^{m} \mathbb{F}_q[x]u_i$ und der Konstruktion von $\tilde{u}$ folgt

$$\mathcal{O}' = \sum_{\substack{i \in \{1, \ldots, m\} \\ i \neq k_1}} \mathbb{F}_q[x]u_i + \mathbb{F}_q[x]\tilde{u}.$$

Daher bilden $u_1, \ldots, u_{k_1-1}, \tilde{u}, u_{k_1+1}, \ldots, u_m$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$.

Schritt 4. Rückkehr zu Schritt 1.

Lemma 3.5.4 *Algorithmus 3.5.3 ist endlich.*

Beweis. Seien $\nu_1, \ldots, \nu_m$ wie am Anfang dieses Abschnitts definiert. Der Input von Algorithmus 3.5.3 sind Ganzheitsbasiselemente $u_1, \ldots, u_m$, die mittels Algorithmus 3.4.6 berechnet worden sind. Wir bezeichnen die Summe ihrer Polordnungen an der Stelle P'_∞ mit

$$S_0 := |v_{P'_\infty}(u_1)| + \cdots + |v_{P'_\infty}(u_m)|.$$

Ein Schleifendurchlauf in Algorithmus 3.5.3 sind die Schritte 1 - 4. Wir bezeichnen nach dem k-ten Schleifendurchlauf mit

$$\left\{u_1^{(k)}, \ldots, u_m^{(k)}\right\}$$

eine Ganzheitsbasis in Schritt 1 und mit

$$S_k$$

die Summe der Polordnungen von $u_1^{(k)}, \ldots, u_m^{(k)}$ an der Stelle P'_∞. Da wir mit jedem Schleifendurchlauf ein neues Element bestimmen, dessen Polordnung an der Stelle P'_∞ kleiner als die Polordnung des ursprünglichen Elements ist, gilt für $k \geq 1$:

$$S_k < S_{k-1}.$$

Da $u_1^{(k)}, \ldots, u_m^{(k)}$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ bilden, folgt für $k \geq 0$

$$S_k > 0.$$

Aus den beiden letzten Ungleichungen folgt, dass ein $k' \in \mathbb{N}$ existiert, so dass der Algorithmus nach dem k'-ten Schleifendurchlauf endet. Nach Theorem 3.5.2 gilt $S_{k'} = \sum_{i=1}^{m} \nu_i$, und der Output ist eine Ganzheitsbasis $u_1^{(k')}, \ldots, u_m^{(k')}$ mit $|v_{P'_\infty}(u_i^{(k')})| = \nu_i$ für $i = 1, \ldots, m$.

□

Theorem 3.5.5 *Mit den Algorithmen 3.4.6 und 3.5.3 ist eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ berechenbar, deren Elemente modulo m paarweise inkongruente Polordnungen an der Stelle P'_∞ haben.*

3.6 Basis des Vektorraums $\boldsymbol{\mathcal{L}\left(rP'_\infty\right)}$

Proposition 3.6.1 *Sei $r \geq 0$. Sei $\{u_1, \ldots, u_m\}$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$, für die $v_{P'_\infty}(u_i) \not\equiv v_{P'_\infty}(u_j)$ mod m für $i, j = 1, \ldots, m$ und $i \neq j$ gilt. Die Elemente $x^j u_i$ mit $0 \leq j$, $1 \leq i \leq m$ und $jm - v_{P'_\infty}(u_i) \leq r$ bilden eine $\mathbb{F}_q$-Basis des Vektorraums $\mathcal{L}(rP'_\infty)$.*

Beweis. Da $\mathcal{O}' = \bigcup_{s\geq 0}^{\infty} \mathcal{L}(sP'_\infty)$, gilt $z \in \mathcal{L}(rP'_\infty) \Longrightarrow z \in \mathcal{O}'$. Damit gilt nach Lemma 2.1.18:

$$\mathcal{L}(rP'_\infty) = \{z \in \mathcal{O}' \mid v_{P'}(z) \geq -v_{P'}(rP'_\infty) \text{ für alle } P' \in \mathbb{P}_{F'}\}.$$

Da für jedes $z \in \mathcal{O}'$ gilt

$$v_{P'}(z) \geq 0 = v_{P'}(rP'_\infty) \qquad \text{für } P' \in \mathbb{P}_{F'} \setminus \{P'_\infty\},$$

schreiben wir $\mathcal{L}(rP'_\infty)$ wie folgt:

$$\mathcal{L}(rP'_\infty) = \left\{z \in \mathcal{O}' \mid v_{P'_\infty}(z) \geq -v_{P'_\infty}(rP'_\infty)\right\} = \left\{z \in \mathcal{O}' \mid v_{P'_\infty}(z) \geq -r\right\}.$$

Da $\mathcal{O}' = \sum_{i=1}^{m} \mathbb{F}_q[x]u_i$, hat jedes $0 \neq z \in \mathcal{O}'$ die Darstellung

$$z = \sum_{i=1}^{m} \sum_{j\geq 0} \gamma_{ij} x^j u_i$$

mit nur endlich vielen $\gamma_{ij} \in \mathbb{F}_q^*$ für $i = 1, \ldots, m$ und $j \geq 0$.

Die Elemente $x^j u_i$ für $i = 1, \ldots, m$ und für $j \geq 0$ haben paarweise inkongruente Polordnungen an der Stelle P'_∞, weil $u_1, \ldots, u_m$ modulo m paarweise inkongruente Polordnungen an der Stelle P'_∞ haben und $v_{P'_\infty}(x) = -m$ gilt. Damit folgt nach Lemma 2.1.8

$$v_{P'_\infty}(z) = min_{ij}\left\{v_{P'_\infty}\left(\gamma_{ij} x^j u_i\right)\right\} = min_{ij}\left\{v_{P'_\infty}\left(x^j u_i\right)\right\}.$$

Damit $z \in \mathcal{L}(rP'_\infty)$, muß $v_{P'_\infty}(z) \geq -r$ gelten. Daher muß für jedes $j \geq 0$ und für jedes $i \in \{1, \ldots, m\}$ gelten:

$$v_{P'_\infty}\left(x^j u_i\right) \geq -r.$$

Daraus folgt die zusätzliche Bedingung für i und j:

$$r \geq jm - v_{P'_\infty}(u_i).$$

□

Wir verfolgen das Ziel, die Berechnung von Basen für $\boldsymbol{\mathcal{L}\left(rP'_\infty\right)}$ zu implementieren. Für die Verkürzung der Rechenzeit des entsprechenden Programms brauchen wir noch zwei wichtige Ergebnisse.

3.7 T-Mengen

Gelten die Voraussetzungen von Abschnitt 3.4, so haben wir für $i = 1, \ldots, m$:

$$w_i^Q = \sum_{j=1}^{m} b_{ij} w_j \quad \text{ mit } b_{ij} \in \mathbb{F}_q(x).$$

Wir definieren Mengen B_i für $i = 1, \ldots, m$

$$B_i := \{j \in \{1, \ldots, m\} \mid b_{ij} \neq 0\}$$

und führen eine Äquivalenzrelation auf der Menge $\{w_1, \ldots, w_m\}$ wie folgt ein:

$$w_i \sim w_j \Longleftrightarrow B_i = B_j.$$

Sei $\bar{m} := |\{w_1, \ldots, w_m\}/\sim|$. Wir wählen eine beliebige Reihenfolge der Äquivalenzklassen, bezeichnen für $t = 1, \ldots, \bar{m}$ mit

$$T_t \text{ die } t\text{-te Äquivalenzklasse}$$

und setzen für $t = 1, \ldots, \bar{m}$

$$\begin{aligned} \tilde{I}_t &:= \{i \in \{1, \ldots, m\} \mid w_i \in T_t\}, \\ J_t &:= \{j \in \{1, \ldots, m\} \mid b_{ij} \neq 0 \text{ für } i \in \tilde{I}_t\}. \end{aligned}$$

Damit gilt $J_t = B_i$ für alle $i \in \tilde{I}_t$, und die Mengen $\tilde{I}_t$ sind paarweise disjunkt für $t = 1, \ldots, \bar{m}$.

Proposition 3.7.1 *Sei $k \in \{2, \ldots, m\}$. Sei $t' \in \{1, \ldots, \bar{m}\}$, so dass $w_k \in T_{t'}$. Sind die Mengen J_t für $t = 1, \ldots, \bar{m}$ paarweise disjunkt, gilt $c_{(i,k)} = 0$ für alle $i \in \{1, \ldots, k-1\} \setminus \tilde{I}_{t'}$. Damit sieht u_k nach dem Ablauf des Algorithmus 3.4.6 wie folgt aus:*

$$u_k = \sum_{i \in \tilde{I}_{t'} \cap \{1, \ldots, k\}} c_{(i,k)} w_i.$$

Beweis. Wir fixieren ein $k \in \{2, \ldots, m\}$ und verfolgen Algorithmus 3.4.6 ab Schritt 2 unter den Voraussetzungen der Proposition.

Da $\{1, \ldots, m\} = \dot{\bigcup}_{t=1}^{\bar{m}} J_t$ gilt, hat $z(e_1, \ldots, e_l)^Q$ in (9) in Schritt 2.2 folgende Darstellung:

$$z(e_1, \ldots, e_l)^Q = \sum_{t=1}^{\bar{m}} \left(\sum_{j \in J_t} \left(\frac{\displaystyle\sum_{i \in \tilde{I}_t \cap \{1, \ldots, k\}} \sum_{s=0}^{l_i} e_{\phi(i,s)} x^{sQ} b''_{ij}}{kgV(d_{1j}, \ldots, d_{kj})} \right) w_j \right)$$

mit $b''_{ij} = b_{ij} \cdot kgV(d_{1j}, \ldots, d_{kj}) \in \mathbb{F}_q[x]$ für $i \in \tilde{I}_t \cap \{1, \ldots, k\}$, für $j \in J_t$ und für $t = 1, \ldots, \bar{m}$. Mit dem gleichen Verfahren wie in Schritt 2.2 muß analog zu (10) für $t = 1, \ldots, \bar{m}$ und für $j \in J_t$ gelten:

$$\left(\frac{\displaystyle\sum_{i \in \tilde{I}_t \cap \{1, \ldots, k\}} \sum_{s=0}^{l_i} e_{\phi(i,s)} x^{sQ} b''_{ij}}{kgV(d_{1j}, \ldots, d_{kj})} \right) \in \mathbb{F}_q(e_1, \ldots, e_l)[x].$$

Wir schreiben das Tupel $e = (e_1, \ldots, e_l)$ koordinatenweise so um, dass zuerst $e_{\phi(i,s)}$ mit $i \in \tilde{I}_1 \cap \{1, \ldots, k\}$, dann $e_{\phi(i,s)}$ mit $i \in \tilde{I}_2 \cap \{1, \ldots, k\}$ und so weiter bis einschließlich $e_{\phi(i,s)}$ mit $i \in \tilde{I}_{\bar{m}} \cap \{1, \ldots, k\}$ nacheinander darin vorkommen.[8] Damit sieht das lineare Gleichungssystem (12) aus Schritt 2.2 wie folgt aus:

$$\begin{pmatrix} \left(S^{(1)} \times L^{(1)} \right) & (0) & \cdots & (0) \\ (0) & \left(S^{(2)} \times L^{(2)} \right) & \cdots & (0) \\ \vdots & \vdots & \vdots & \vdots \\ (0) & (0) & \cdots & \left(S^{(\bar{m})} \times L^{(\bar{m})} \right) \end{pmatrix} \times e^T = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix},$$

wobei jeder Block $\left(S^{(t)} \times L^{(t)}\right)$ für $t = 1, \ldots, \bar{m}$ eine Matrix darstellt mit $S^{(t)} := |J_t| \cdot \sum_{j \in J_t} \left(h_j^{(r_j)} + 1\right)$ Zeilen[9] und mit $L^{(t)} := \sum_{i \in \tilde{I}_t} (l_i + 1)$ Spalten.

Wir wissen nach den Schritten 2.3 und 2.4, dass es im Lösungsraum dieses Systems genau eine nichttriviale Lösung $(e_1^*, \ldots, e_l^*) \in \mathbb{F}_q^l$ gibt, so dass für $i = 1, \ldots, k$ gilt:

$$c_{(i,k)} = a_i(e_1^*, \ldots, e_l^*, x).$$

Da nach der Voraussetzung der Proposition $k \in \tilde{I}_{t'}$ gilt, werden die $c_{(i,k)}$ für $i \in \tilde{I}_{t'} \cap \{1, \ldots, k\}$ und insbesondere der Idealerzeuger $c_{(k,k)} \neq 0$ durch den Block $\left(S^{(t')} \times L^{(t')}\right)$ des Systems bestimmt. Wegen der Eindeutigkeit der Lösung $(e_1^*, \ldots, e_l^*)$, und da dieses lineare Gleichungssystem homogen ist, folgt $e_{\phi(i,s)}^* = 0$ für $i \in \{1, \ldots, k-1\} \setminus \tilde{I}_{t'}$ und für $s = 0, \ldots, l_i$. Damit sind die $c_{(i,k)} = 0$ für $i \in \{1, \ldots, k-1\} \setminus \tilde{I}_{t'}$.

□

Erfüllt die in Abschnitt 3.1(2) gewählte Basis $\{w_1, \ldots, w_m\}$ die Voraussetzung von Proposition 3.7.1, setzen wir in Algorithmus 3.4.6 in Schritt 2.2 (siehe (8)) für $i \in \{1, \ldots, k-1\} \setminus \tilde{I}_{t'}$: $a_i(e_1, \ldots, e_l, x) := 0$. Damit wird die Division in (10) in Schritt 2.2 nur für die $j \in J_{t'}$ durchgeführt.

3.8 Ablauf der Algorithmen 3.4.6 und 3.5.3 über $\mathbb{F}_p$

Da die Algorithmen 3.4.6 und 3.5.3 zu den Berechnungen von Ganzheitsbasen für $F'/\mathbb{F}_q(x)$ geschrieben worden sind, finden alle Berechnungen natürlicherweise über $\mathbb{F}_q$ statt. Insbesondere wird $Q = q^{n_1}$ für ein $n_1 \in \mathbb{N}$ gewählt. Wir werden in diesem Abschnitt zeigen, dass es unter gewissen Voraussetzungen möglich ist, alle Berechnungen über $\mathbb{F}_p$ durchzuführen und trotzdem eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ zu bestimmen. Dabei werden wir $Q = p^{n_2}$ für ein $n_2 \in \mathbb{N}$ wählen.[10]

[8] Sei zum Beispiel $\tilde{I}_t \cap \{1, \ldots, k\} = \{i_1, \ldots, i_s\}$ für ein $t \in \{1, \ldots, \bar{m}\}$. Damit ist

$$e = \Big(\underbrace{e_{\phi(i,0)}, \cdots}_{i \in \tilde{I}_1 \cap \{1,\ldots,k\}}, \ldots, \underbrace{e_{\phi(i_1,0)}, \ldots, e_{\phi(i_1,l_{i_1})}, \ldots, e_{\phi(i_s,0)}, e_{\phi(i_s,l_{i_s})}}_{\text{für } \tilde{I}_t \cap \{1,\ldots,k\}}, \ldots, \underbrace{\ldots, e_{\phi(i,l_i)}}_{i \in \tilde{I}_{\bar{m}} \cap \{1,\ldots,k\}} \Big).$$

[9] r_j ist auf Seite 24 definiert.

[10] Dies verkürzt die Rechenzeit des Algorithmus 3.4.6. So sei zum Beispiel $q = 27$ und $v_{P'}(w_i) > -7$ für alle $P' \in \mathbb{P}_{F'} \setminus \{P'_\infty\}$ und für $i = 1, \ldots, m$. Laut Algorithmus 3.4.6 wählen wir $Q = 27$ mit $n_1 = 1$. Gelten jedoch die nötigen Voraussetzungen, können wir über $\mathbb{F}_p$ rechnen. So werden wir dann $Q = 9$ mit $n_2 = 2$ wählen. Es macht einen Unterschied, ob die Basisdarstellungen von w_i^{27} oder von w_i^9 für $i = 1, \ldots, m$ berechnet werden müssen.

Sei $L/\mathbb{F}_p$ ein algebraischer Funktionenkörper mit dem Konstantenkörper $\mathbb{F}_p$, so dass $F' = L\mathbb{F}_q$ eine algebraische Konstantenkörpererweiterung von $L/\mathbb{F}_p$ ist. Nach Proposition 2.2.10(2) ist $\mathbb{F}_q$ der volle Konstantenkörper von $F'/\mathbb{F}_q$. Nach Proposition 2.2.10(1) ist $L/\mathbb{F}_p(x)$ eine endliche Funktionenkörpererweiterung vom Grad m. Da $F'/\mathbb{F}_q(x)$ und $\mathbb{F}_q(x)/\mathbb{F}_p(x)$ separabel sind, ist $L/\mathbb{F}_p(x)$ ebenso separabel.

Sei Q_∞ der Pol von x in $\mathbb{F}_p(x)$. Da P_∞ voll verzweigt in $F'/\mathbb{F}_q(x)$ ist, und da nach Proposition 2.2.10(3) jede Stelle von $L/\mathbb{F}_p$ unverzweigt in F'/L ist, bzw. jede Stelle von $\mathbb{F}_p(x)/\mathbb{F}_p$ unverzweigt in $\mathbb{F}_q(x)/\mathbb{F}_p(x)$ ist, folgt nach Proposition 2.2.11, dass Q_∞ voll verzweigt in $L/\mathbb{F}_p(x)$ ist. Daher existiert genau eine Stelle $Q'_\infty \in \mathbb{P}_L$ mit $O'_\infty | Q_\infty$.

Sei $\mathcal{O}_L := \{z \in L \mid v_{Q'}(z) \geq 0 \text{ für alle } Q' \in \mathbb{P}_L \setminus \{Q'_\infty\}\}$.

Sei $g(L)$ das Geschlecht von $L/\mathbb{F}_p$.

Sei $g(F')$ das Geschlecht von $F'/\mathbb{F}_q$.

Lemma 3.8.1 *Gelte die obige Situation und sei $\alpha \in \mathbb{N} \cup \{0\}$. Dann ist α eine Polzahl von P'_∞ dann und nur dann, wenn α eine Polzahl von Q'_∞ ist.*

Beweis. $\Longleftarrow$ Sei α eine Polzahl von Q'_∞. Nach Lemma 3.5.1(2) existiert ein $z \in \mathcal{O}_L$ mit $v_{Q'_\infty}(z) = -\alpha$. Wegen $\mathcal{O}_L \subseteq \mathcal{O}'$ und $e(P'_\infty | Q'_\infty) = 1$ gilt: $z \in \mathcal{O}'$ mit $v_{P'_\infty}(z) = -\alpha$. Dann ist nach Lemma 3.5.1(2) α eine Polzahl von P'_∞.

$\Longrightarrow$ Sei α eine Polzahl von P'_∞, aber eine Fehlzahl von Q'_∞. Nach "$\Longleftarrow$" folgt: jede Fehlzahl von P'_∞ ist eine Fehlzahl von Q'_∞. Damit gilt wegen α

$$\{\beta \mid \beta \text{ ist eine Fehlzahl von } P'_\infty\} \subsetneqq \{\gamma \mid \gamma \text{ ist eine Fehlzahl von } Q'_\infty\}.$$

Daraus folgt nach Theorem 2.1.21

$$g(F') < g(L).$$

Nach Proposition 2.2.10(4) gilt jedoch

$$g(F') = g(L).$$

Damit folgt, dass α eine Polzahl auch von Q'_∞ ist.

□

Proposition 3.8.2 *Gelte die obige Situation. Dann ist jede Ganzheitsbasis für $L/\mathbb{F}_p(x)$ mit Elementen, deren Polordnungen an der Stelle Q'_∞ modulo m paarweise inkongruent sind, eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ mit Elementen, deren Polordnungen an der Stelle P'_∞ ebenso modulo m paarweise inkongruent sind.*

Beweis. Sei $\{y_1, \ldots, y_m\}$ eine Ganzheitsbasis für $L/\mathbb{F}_p(x)$, so dass für $i \neq j$ und $i, j = 1, \ldots, m$ gilt: $v_{Q'_\infty}(y_i) \not\equiv v_{Q'_\infty}(y_j) \; mod \; m$. Nach Theorem 3.5.2 gilt für $i = 1, \ldots, m$:

$$v_{Q'_\infty}(y_i) = min\{\alpha \in \mathbb{N} \mid \alpha \text{ ist eine Polzahl von } Q'_\infty \text{ mit } \alpha \equiv i \; mod \; m\}.$$

Wegen $\mathcal{O}_L \subseteq \mathcal{O}'$ gilt $y_1, \ldots, y_m \in \mathcal{O}'$, und wegen $e(P'_\infty | Q'_\infty) = 1$ gilt für $i = 1, \ldots, m$

$$v_{P'_\infty}(y_i) = v_{Q'_\infty}(y_i).$$

Damit und nach Lemma 3.8.1 folgt

$$v_{P'_\infty}(y_i) = min\{\alpha \in \mathbb{N} \mid \alpha \text{ ist eine Polzahl von } P'_\infty \text{ mit } \alpha \equiv i \ mod \ m\}.$$

Nach Theorem 3.5.2 ist $\{y_1, \ldots, y_m\}$ eine Ganzheitsbasis für $F'/\mathbb{F}_q(x)$ mit $v_{P'_\infty}(y_i) \not\equiv v_{P'_\infty}(y_j) \ mod \ m$ für $i, j = 1, \ldots, m$ und $i \neq j$.

□

3.9 Ein Algorithmus zur Berechnung einer Basis von $\mathcal{L}(rP'_\infty)$

Unter den Voraussetzungen aus den Abschnitten 3.1 und 3.4 und mit den Ergebnissen des Kapitels 3 können Basen von $\mathcal{L}(rP'_\infty)$ wie folgt berechnet werden.

Algorithmus 3.9.1 *Berechnung einer Basis von $\mathcal{L}(rP'_\infty)$ für ein $r \geq 0$.*

Schritt 1 Wir wählen wie in Abschnitt 3.1(2) eine Basis $\{w_1, \ldots, w_m\}$ für $F'/\mathbb{F}_q(x)$. Wir nehmen an, dass $v_{P'_\infty}(w_i) \not\equiv v_{P'_\infty}(w_j) \ mod \ m$ für $i, j = 1, \ldots, m$ und $i \neq j$ gilt.

Schritt 2 Wir wählen wie in Abschnitt 3.1(4) eine Zahl $Q \in \mathbb{N}$, so dass $Q = q^{n_1}$ für ein $n_1 \in \mathbb{N}$.

Schritt 3 Wir bestimmen für $i = 1, \ldots, m$:

$$w_i^Q = \sum_{j=1}^{m} b_{ij} w_j \text{ mit } b_{ij} \in \mathbb{F}_q(x) \text{ für } i, j = 1, \ldots, m.$$

Zu den Schritten 1-3 ist noch folgendes zu sagen: wie wir die Basis $\{w_1, \ldots, w_m\}$ und die Zahl Q wählen und die Basisdarstellungen von $w_1^Q, \ldots, w_m^Q$ bestimmen, hängt von der Struktur von $F'/\mathbb{F}_q(x)$ ab.

Schritt 4 Wir definieren nach (4) in Abschnitt 3.4 die Polynome D_i für $i = 1, \ldots, m$. Siehe dazu auch Lemma 3.4.2 und Folgerung 3.4.3.

Schritt 5 Wir definieren wie in Abschnitt 3.7 Mengen T_t für $t = 1, \ldots, \bar{m}$. Wir testen, ob ihre Indexmengen J_t für $t = 1, \ldots, \bar{m}$ paarweise disjunkt sind.

Schritt 6 Wir berechnen eine Ganzheitsbasis $\{u_1, \ldots, u_m\}$ für $F'/\mathbb{F}_q(x)$ mittels Algorithmus 3.4.6. Dabei ist zu beachten: sind J_t für $t = 1, \ldots, \bar{m}$ nicht paarweise disjunkt, verläuft Algorithmus 3.4.6 exakt nach seiner Beschreibung. Sind J_t für $t = 1, \ldots, \bar{m}$ jedoch paarweise disjunkt, fixieren wir vor Schritt 2.2 den Index $t' \in \{1, \ldots \bar{m}\}$, für den $w_k \in T_{t'}$ gilt. Nach Proposition 3.7.1 werden $a_i(e_1, \ldots, e_l, x) := 0$ (in (8) in Schritt 2.2) für $i \in \{1, \ldots, k-1\} \setminus \tilde{I}_{t'}$ gesetzt.

Schritt 7 Wir bestimmen mittels Algorithmus 3.5.3 eine Ganzheitsbasis $\{u_1^*, \ldots, u_m^*\}$ für $F'/\mathbb{F}_q(x)$, deren Elemente modulo m paarweise inkongruente Polordnungen an der Stelle P'_∞ haben.

Schritt 8 Wir berechnen nach Proposition 3.6.1 eine Basis des Vektorraums $\mathcal{L}(rP'_\infty)$.

Gelten die Voraussetzungen aus Abschnitt 3.8, so wählen wir in Schritt 1 eine Basis $\{w_1, \ldots, w_m\}$ für $F'/\mathbb{F}_q(x)$, allerdings über $\mathbb{F}_p$, und in Schritt 2 die Zahl $Q = p^{n_2}$ für ein $n_2 \in \mathbb{N}$. Damit werden alle Berechnungen in Algorithmus 3.9.1 über $\mathbb{F}_p$ stattfinden.

Im nächsten Kapitel werden wir einen Turm $(F_n)_{n \geq 0}$ algebraischer Funktionenkörper betrachten, für den Algorithmus 3.9.1 angewendet wird.

4 Globale Ganzheitsbasen in einem Turm $(F_n)_{n\geq 0}$ algebraischer Funktionenkörper und Basen für die Vektorräume $\mathcal{L}\left(rP_\infty^{(n)}\right)$

4.1 Vorbereitungen

Sei $\mathbb{F}_{p^2}$ der endliche Körper mit p^2 Elementen und Charakteristik $p > 2$, p ist Primzahl.

Sei $\mathcal{F} = (F_0, F_1, \ldots, F_n, \ldots)$ der wie folgt definierte Funktionenkörperturm:

$$F_0 = \mathbb{F}_{p^2}(x_0),$$

wobei x_0 transzendent über $\mathbb{F}_{p^2}$ ist, und

$$F_n = F_{n-1}(x_n) \text{ für } n \geq 1,$$

wobei x_n die folgende Gleichung erfüllt

$$x_n^2 = \frac{x_{n-1}^2 + 1}{2x_{n-1}}. \tag{25}$$

Da $F_0/\mathbb{F}_{p^2}$ rational ist, bezeichnen wir mit P_∞ den einzigen Pol von x_0 in F_0 und mit $P_\alpha \in \mathbb{P}_{F_0}\backslash\{P_\infty\}$ die Stelle von $F_0/\mathbb{F}_{p^2}$, der das Polynom $x_0 - \alpha \in \mathbb{F}_{p^2}[x_0]$ entspricht. Nach Definition ist P_α die Nullstelle des Elements $x_0 - \alpha$ in F_0.

Nach Proposition 5.3 [Gar-Sti-Rüc] ist der Verzweigungsort dieses Turms

$$V(\mathcal{F}) = \{P_1, P_{-1}, P_{-I}, P_I, P_0, P_\infty\},$$

wobei $I \in \mathbb{F}_{p^2}$ mit $I^2 = -1$ ist.

Bemerkung 4.1.1 *Nach dem Beweis von Proposition 5.3 [Gar-Sti-Rüc] gilt: die Stellen P_0, $P_{\pm I}$, P_∞ sind voll verzweigt in $\mathcal{F}$, und die Stelle P_{-1} ist voll verzweigt in $\mathcal{F}$ ab dem Funktionenkörper F_2. Die Verzweigung über der Stelle P_1 ist komplexer und wird in Kürze genauer diskutiert.*

Wir definieren:

$$\mathcal{S}_0 := \mathbb{P}_{F_0} \setminus \{P_\infty\},$$

$$\mathcal{O}_0 := \bigcap_{P \in \mathcal{S}_0} \mathcal{O}_P = \mathbb{F}_{p^2}[x_0] \subseteq F_0.$$

Sei $n \geq 1$. Nach Bemerkung 4.1.1 existiert genau eine Stelle von $F_n/\mathbb{F}_{p^2}$, die über $P_\infty \in \mathbb{P}_{F_0}$ liegt. Diese bezeichnen wir mit $P_\infty^{(n)}$. Damit definieren wir:

$$\mathcal{S}_n := \mathbb{P}_{F_n} \setminus \left\{P_\infty^{(n)}\right\},$$

$$\mathcal{O}_n := ic_{F_n}(\mathcal{O}_0) \subseteq F_n.$$

Die Stellen aus $\mathcal{S}_n$ bezeichnen wir mit $P^{(n)}$. Nach Proposition 2.2.14 gilt:

$$\mathcal{O}_n = \bigcap_{P^{(n)} \in \mathcal{S}_n} \mathcal{O}_{P^{(n)}} = \left\{z \in F_n \mid v_{P^{(n)}}(z) \geq 0 \text{ für alle } P^{(n)} \in \mathcal{S}_n\right\}.$$

Sei $P^{(n)} \in \mathcal{S}_n$ und $i \in \{1, \ldots, n\}$. Da $F_n/\mathbb{F}_{p^2}(x_i)$ eine Funktionenkörpererweiterung ist, existiert nach Proposition 2.2.4 genau eine Stelle $Q^{(i)} \in \mathbb{P}_{\mathbb{F}_{p^2}(x_i)}$, so dass $P^{(n)} \cap \mathbb{F}_{p^2}(x_i) = Q^{(i)}$. Ist *deg* $Q^{(i)} = 1$ und
i) ist $Q^{(i)}$ kein Pol von x_i in $\mathbb{F}_{p^2}(x_i)$, dann existiert genau ein $\alpha \in \mathbb{F}_{p^2}$, so dass $< x_i - \alpha >= Q^{(i)}$, und wir schreiben $x_i\left(P^{(n)}\right) = \alpha$.
ii) ist $Q^{(i)}$ der Pol von x_i in $\mathbb{F}_{p^2}(x_i)$, so schreiben wir $x_i(P^{(n)}) = \infty$.
Im Fall $P^{(n)} \cap F_0 \in \left\{P_\alpha \mid \alpha \in \mathbb{F}_{p^2}\right\} \cup \{P_\infty\}$ schreiben wir jeweils $x_0\left(P^{(n)}\right) = \alpha$ und $x_0\left(P^{(n)}\right) = \infty$.

Bemerkung 4.1.2 *Aus der Gleichung (25) folgt: für alle $t \in \mathbb{N}$, $t \geq 2$ existieren mindestens zwei Stellen $P_1^{(t)}$ und $P_2^{(t)}$ von $F_t/\mathbb{F}_{p^2}$, so dass*

$$x_t\left(P_i^{(t)}\right) = (-1)^i I \text{ und } P_i^{(t)} \cap F_0 = P_1 \text{ für } i = 1, 2.$$

Sei $i \in \{1, 2\}$. Dann gilt:
1. $x_j\left(P_i^{(t)}\right) = 1$ für $j = 0, \ldots, t-2$.
2. $x_{t-1}\left(P_i^{(t)}\right) = -1$.
3. Für alle $P^{(t+1)} \in \mathcal{S}_{t+1}$ mit $P^{(t+1)} \cap F_t = P_i^{(t)}$ gilt: $x_{t+1}\left(P^{(t+1)}\right) = 0$.
4. Sei $j \geq t+2$. Dann gilt für alle $P^{(j)} \in \mathcal{S}_j$ mit $P^{(j)} \cap F_t = P_i^{(t)}$: $x_j\left(P^{(j)}\right) = \infty$.

Fixieren wir ein $t \geq 2$ aus Bemerkung 4.1.2, so sind die Verzweigungsindizes der Einschränkungen und der Fortsetzungen von $P_i^{(t)}$ für $i = 1, 2$ aus der folgenden Abbildung 1 abzulesen:

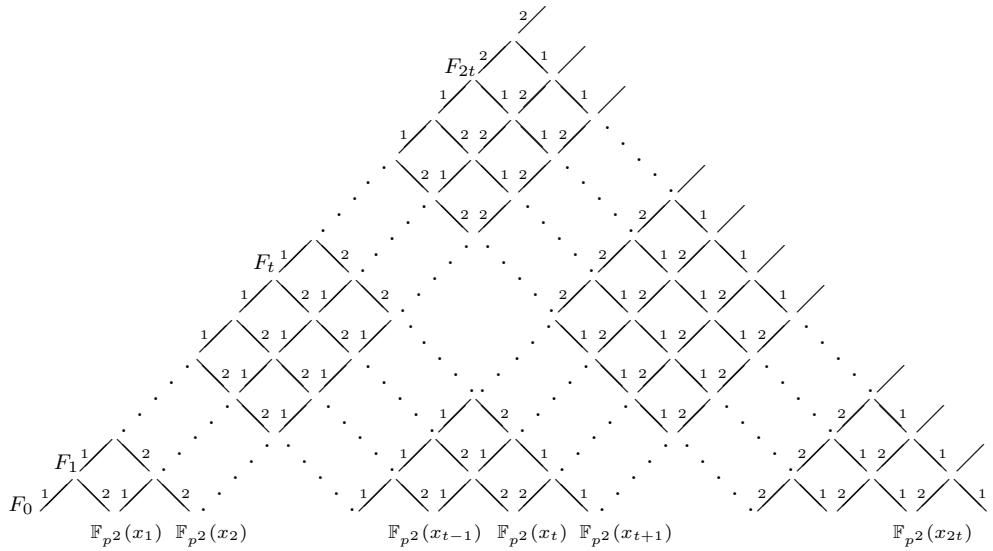


Abbildung 1.

Damit ist die Verzweigung über $P_1 \in \mathcal{S}_0$ beschrieben.

Sei $n \geq 1$. Wir assoziieren zu jeder Stelle $P^{(n)} \in \mathcal{S}_n$ eine Zahl $s \in \mathbb{Z}$ mit $-1 \leq s \leq n+3$ wie folgt:

$$\begin{array}{lll}
s=-1, & \text{falls } P^{(n)} \cap F_0 = P_0, & \\
s=0, & \text{falls } P^{(n)} \cap F_0 = P_{\pm I}, & \\
s=1, & \text{falls } P^{(n)} \cap F_0 = P_{-1}, & \\
s=t, & \text{falls } P^{(n)} \cap F_0 = P_1, \quad x_t\left(P^{(n)}\right) = \pm I & \text{für } t=2,\ldots,n, \quad (n\geq 2) \\
s=n+1, & \text{falls } P^{(n)} \cap F_0 = P_1, \quad x_n\left(P^{(n)}\right) = -1, & \\
s=n+2, & \text{falls } P^{(n)} \cap F_0 = P_1, \quad x_n\left(P^{(n)}\right) = 1, & \\
s=n+3, & \text{falls } P^{(n)} \cap F_0 = P \in \mathcal{S}_0 \setminus V(\mathcal{F}). &
\end{array}$$

Lemma 4.1.3 *Sei s wie oben definiert, dann gilt für $n \geq 1$*

$$v_{P^{(n)}}(x_0^2+1) = \begin{cases} 2^n, & s=0 \\ 0, & s\neq 0 \end{cases}$$

$$v_{P^{(n)}}(x_0+1) = \begin{cases} \begin{cases} 1, & n=1,2, \\ 2^{n-2}, & n\geq 3, \end{cases} & s=1 \\ 0, & s\neq 1 \end{cases}$$

$$v_{P^{(n)}}(x_0-1) = \begin{cases} 0, & s\in\{-1,0,1,n+3\} \\ 2^{n-2s}, & 2\leq s<\frac{n}{2} \\ 1, & \frac{n}{2}\leq s\leq n+2 \end{cases}$$

und für $i=0,\ldots,n$

$$v_{P^{(n)}}(x_i) = \begin{cases} \begin{cases} 0, & i<s+1, \\ 2^{n-i}, & i=s+1, \\ -2^{n-i}, & i>s+1, \end{cases} & -1\leq s<\frac{n}{2} \\ \begin{cases} 0, & i<s+1, \\ 2^{s-1}, & i=s+1, \\ -2^{2s-i}, & i>s+1, \end{cases} & \frac{n}{2}\leq s<n \\ 0, & n\leq s\leq n+3 \end{cases}$$

Beweis. Sei $P^{(n)} \in \mathcal{S}_n$. Dann existiert genau eine Stelle $P \in \mathcal{S}_0$, so dass $P^{(n)}|P$ und für $z \in F_0$ gilt:

$$v_{P^{(n)}}(z) = e(P^{(n)}|P)v_P(z). \tag{26}$$

Sei $z = x_0^2+1 = (x_0+I)(x_0-I)$. Nach Bemerkung 4.1.1 ist $P_{\pm I}$ voll verzweigt in $\mathcal{F}$ und nach Definition ist $x_0 \mp I \in \mathbb{F}_{p^2}[x_0]$ ein Primelement für diese Stelle. Damit gilt nach (26):

$$v_{P^{(n)}}(x_0^2+1) = \begin{cases} e(P^{(n)}|P), & P=P_{\pm I} \\ 0, & P\neq P_{\pm I} \end{cases} = \begin{cases} 2^n, & s=0 \\ 0, & s\neq 0 \end{cases}$$

Sei $z = x_0+1$. Nach Bemerkung 4.1.1 ist P_{-1} voll verzweigt in $\mathcal{F}$ ab dem Funktionenkörper F_2, und nach der definierenden Gleichung (25) ist sie unverzweigt in F_2/F_0. Nach Definition ist $x_0+1 \in \mathbb{F}_{p^2}[x_0]$ ein Primelement für diese

Stelle. Damit folgt nach (26):

$$v_{P^{(n)}}(x_0+1) = \begin{cases} e(P^{(n)}|P), & P = P_{-1} \\ 0, & P \neq P_{-1} \end{cases} = \begin{cases} \begin{cases} 1, & n = 1,2, \\ 2^{n-2}, & n \geq 3, \end{cases} & s = 1 \\ 0, & s \neq 1 \end{cases}$$

Sei $z = x_0 - 1$. Nach Definition ist $x_0 - 1 \in \mathbb{F}_{p^2}[x_0]$ ein Primelement für P_1. Dann folgt nach (26) und Abbildung 1:

$$v_{P^{(n)}}(x_0-1) = \begin{cases} e(P^{(n)}|P), & P = P_1 \\ 0, & P \neq P_1 \end{cases} = \begin{cases} 2^{n-2s}, & 2 \leq s < \frac{n}{2} \\ 1, & \frac{n}{2} \leq s \leq n+2 \\ 0, & s \in \{-1, 0, 1, n+3\} \end{cases}$$

Nun berechnen wir $v_{P^{(n)}}(x_i)$ für $i = 0, \ldots, n$ und für alle $P^{(n)} \in \mathcal{S}_n$. Nach (26) gilt:

$$v_{P^{(n)}}(x_0) = e(P^{(n)}|P) v_P(x_0). \tag{27}$$

Für jede Stelle $P^{(n)} \in \mathcal{S}_n$ existiert genau eine Stelle $P^{(i)} \in \mathcal{S}_i$, so dass $P^{(n)} \cap F_i = P^{(i)}$ für $i = 1, \ldots, n-1$, und für diese existiert genau eine Stelle $Q^{(i)} \in \mathbb{P}_{\mathbb{F}_{p^2}(x_i)}$ mit $P^{(i)} \cap F_{p^2(x_i)} = Q^{(i)}$ für $i = 1, \ldots, n$. Damit gilt für $i = 1, \ldots, n-1$

$$v_{P^{(n)}}(x_i) = e(P^{(n)}|P^{(i)}) e(P^{(i)}|Q^{(i)}) v_{Q^{(i)}}(x_i) \tag{28}$$

und

$$v_{P^{(n)}}(x_n) = e(P^{(n)}|Q^{(n)}) v_{Q^{(n)}}(x_n). \tag{29}$$

Es gilt für $i = 1, \ldots, n$: $v_{Q^{(i)}}(x_i) \neq 0 \iff Q^{(i)}$ ist die Nullstelle oder der Pol von x_i in $\mathbb{F}_{p^2}(x_i)$. Ist $Q^{(i)}$ die Nullstelle von x_i in $\mathbb{F}_{p^2}(x_i)$, gilt $x_i(P^{(n)}) = 0$ und $v_{Q^{(i)}}(x_i) = 1$. Ist $Q^{(i)}$ der Pol von x_i in $\mathbb{F}_{p^2}(x_i)$, gilt $x_i(P^{(n)}) = \infty$ und $v_{Q^{(i)}}(x_i) = -1$.

Wir unterscheiden weiter fünf Fälle, je nachdem, welche Stelle $P^{(n)} \cap F_0$ ist.

1. Sei $P^{(n)} \cap F_0 = P_0$. Damit folgt aus der Gleichung (25) $x_0(P^{(n)}) = 0$ und $x_i(P^{(n)}) = \infty$ für $i = 1, \ldots, n$. Nach Bemerkung 4.1.1 ist P_0 voll verzweigt in $\mathcal{F}$, und nach der Gleichung (25) ist die Stelle $P^{(i)} \in \mathcal{S}_i$ mit $P^{(i)} \cap F_0 = P_0$ unverzweigt in $F_i/\mathbb{F}_{p^2}(x_i)$ für $i \geq 1$. Damit und nach (27) - (29) folgt für $i = 0, \ldots, n$ ($s = -1$):

$$\begin{aligned} v_{P^{(n)}}(x_i) &= \begin{cases} e(P^{(n)}|P_0) v_{P_0}(x_0), & i = 0 \\ e(P^{(n)}|P^{(i)}) e(P^{(i)}|Q^{(i)}) v_{Q^{(i)}}(x_i), & i = 1, \ldots, n-1 \\ e(P^{(n)}|Q^{(n)}) v_{Q^{(n)}}(x_n), & i = n \end{cases} \\ &= \begin{cases} 2^n, & i = 0 \\ 2^{n-i} \cdot (-1), & i = 1, \ldots, n \end{cases} \\ &= \begin{cases} 2^{n-i}, & i = s+1, \\ -2^{n-i}, & i > s+1, \end{cases} \quad s = -1 \end{aligned}$$

2. Sei $P^{(n)} \cap F_0 = P_{\pm I}$. Dann folgt aus der Gleichung (25) $x_0(P^{(n)}) = \pm I$, $x_1(P^{(n)}) = 0$ und $x_i(P^{(n)}) = \infty$ für $i = 2, \ldots, n$. Nach Bemerkung 4.1.1 ist $P_{\pm I}$ voll verzweigt in $\mathcal{F}$, und nach der Gleichung (25) ist die Stelle $P^{(i)} \in \mathcal{S}_i$ mit

$P^{(i)} \cap F_0 = P_{\pm I}$ unverzweigt in $F_i/\mathbb{F}_{p^2}(x_i)$ für $i \geq 1$. Damit und nach (27) - (29) folgt für $i = 0, \ldots, n$ $(s = 0)$:

$$v_{P^{(n)}}(x_i) = \begin{cases} 0, & i = 0 \\ 2^{n-1}, & i = 1 \\ -2^{n-i}, & i = 2, \ldots, n \end{cases} = \begin{cases} 0, & i < s+1, \\ 2^{n-i}, & i = s+1, \\ -2^{n-i}, & i > s+1, \end{cases} \quad s = 0$$

3. Sei $P^{(n)} \cap F_0 = P_{-1}$. Dann folgt aus der definierenden Gleichung (25) $x_0(P^{(n)}) = -1$, $x_1(P^{(n)}) = \pm I$, $x_2(P^{(n)}) = 0$ und $x_i(P^{(n)}) = \infty$ für $i = 3, \ldots, n$. Nach Bemerkung 4.1.1 ist P_{-1} voll verzweigt in $\mathcal{F}$ ab dem Funktionenkörper F_2 und unverzweigt in F_2/F_0. Nach der Gleichung (25) ist jede Stelle $P^{(i)} \in \mathcal{S}_i$ mit $P^{(i)} \cap F_0 = P_{-1}$ unverzweigt in $F_i/\mathbb{F}_{p^2}(x_i)$ für $i \geq 2$, und jede Stelle $P^{(1)} \in \mathcal{S}_1$ mit $P^{(1)} \cap F_0 = P_{-1}$ ist voll verzweigt in $F_1/\mathbb{F}_{p^2}(x_1)$. Damit und nach (27) - (29) folgt für $i = 0, \ldots, n$ $(s = 1)$:

$$v_{P^{(n)}}(x_i) = \begin{cases} 0, & i = 0, 1 \\ 2^{n-2}, & i = 2 \\ -2^{n-i}, & i = 3, \ldots, n \end{cases} = \begin{cases} 0, & i < s+1, \\ 2^{n-i}, & i = s+1, \\ -2^{n-i}, & i > s+1, \end{cases} \quad s = 1$$

4. Sei $P^{(n)} \cap F_0 = P_1$. Damit ist $s \in \{2, \ldots, n+2\}$. Nach Bemerkung 4.1.2, Abbildung 1 und (27) - (29) gelten die drei folgenden Unterfälle:

4.1. Ist $2 \leq s < \frac{n}{2}$, gilt:

$$\begin{array}{rcl} 0 \leq i < s+1 & \Longleftrightarrow & x_i\left(P^{(n)}\right) \in \{\pm 1, \pm I\} \\ & \Longleftrightarrow & v_{P^{(n)}}(x_i) = 0 \\ i = s+1 & \Longleftrightarrow & x_i\left(P^{(n)}\right) = 0 \\ & \Longleftrightarrow & v_{P^{(n)}}(x_i) = 2^{n-2s} \cdot 2^{s-1} = 2^{n-i} \\ s+1 < i \leq n & \Longleftrightarrow & x_i\left(P^{(n)}\right) = \infty \\ & \Longleftrightarrow & v_{P^{(n)}}(x_i) = 2^{n-2s} \cdot 2^{2s-i} \cdot (-1) = -2^{n-i} \text{ für } i < 2s \\ & & \text{und } v_{P^{(n)}}(x_i) = -2^{n-i} \text{ für } i \geq 2s \end{array}$$

4.2. Ist $\frac{n}{2} \leq s < n$, gilt analog Fall 4.1:

$$\begin{array}{rcl} 0 \leq i < s+1 & \Longleftrightarrow & v_{P^{(n)}}(x_i) = 0 \\ i = s+1 & \Longleftrightarrow & v_{P^{(n)}}(x_i) = 1 \cdot 2^{2s-(s+1)} = 2^{s-1} \\ s+1 < i \leq n & \Longleftrightarrow & v_{P^{(n)}}(x_i) = 2^{2s-i} \cdot (-1) = -2^{2s-i} \end{array}$$

4.3. Ist $n \leq s \leq n+2$, gilt $x_i\left(P^{(n)}\right) \in \{\pm 1, \pm I\}$, und damit $v_{P^{(n)}}(x_i) = 0$ für $i = 0, \ldots, n$.

5. Nach dem Beweis von Proposition 5.3 [Gar-Sti-Rüc] folgt für $i = 0, \ldots, n$:

$$x_i(P^{(n)}) \in \{0, \infty\} \Longrightarrow P^{(n)} \cap F_0 = P \in V(\mathcal{F}).$$

Daher gilt $v_{P^{(n)}}(x_i) = 0$ für $P^{(n)} \in \mathcal{S}_n$ mit $P^{(n)} \cap F_0 = P \in \mathcal{S}_0 \setminus V(\mathcal{F})$ und für $i = 0, \ldots, n$. Dabei ist $s = n+3$.

Wenn wir alle fünf Fälle zusammenfassen, bekommen wir die Aussage des Lemmas.

□

4.2 Eine Basis für F_n/F_0 nach Punkt (2) in Abschnitt 3.1

Wir setzen

$$\begin{aligned} \alpha_1 &:= \frac{x_1}{x_0^2+1}, \\ \alpha_2 &:= \frac{x_2}{x_0+1}, \\ \alpha_i &:= \frac{x_i}{(x_0-1)^{2^{i-2}}} \text{ für } i = 3, \ldots, n, \end{aligned} \tag{30}$$

und

$$\beta_i := \frac{1}{\alpha_i} \text{ für } i = 1, \ldots, n.$$

Wir definieren für $n \geq 1$

$$\mathcal{N} := \{1, \ldots, n\},$$
$$m := 2^n.$$

Da $|\{V \mid V \subseteq \mathcal{N}\}| = m$, existiert eine Bijektion $\theta : \{1, \ldots, m\} \to \{V \mid V \subseteq \mathcal{N}\}$. Wir setzen für $j = 1, \ldots, m$

$$V_j := \theta(j) \tag{31}$$

und damit

$$w_j := \prod_{i \in V_j} \alpha_i. \tag{32}$$

Wir werden weiter schreiben

$$\alpha_i \mid w_j \Longleftrightarrow i \in V_j.$$

Sei $n \geq 1$. Nun berechnen wir $v_{P_\infty^{(n)}}(w_j)$ für $j = 1, \ldots, m$. Da $P_\infty \in \mathbb{P}_{F_0}$ voll verzweigt in $\mathcal{F}$ ist, und da nach der Gleichung (25) die Stelle $P^{(i)} \in \mathcal{S}_i$ mit $P^{(i)} \cap F_0 = P_0$ unverzweigt in $F_i/\mathbb{F}_{p^2}(x_i)$ für $i \geq 1$ ist, folgt $v_{P_\infty^{(n)}}(x_i) = -2^{n-i}$ für $i = 0, \ldots, n$. Daher gilt für $j = 1, \ldots, m$:

$$\begin{aligned} v_{P_\infty^{(n)}}(w_j) &= v_{P_\infty^{(n)}}\left(\prod_{i \in V_j} \alpha_i\right) = \sum_{i \in V_j} v_{P_\infty^{(n)}}(\alpha_i) \\ &= \sum_{i=1}^{n} \left(-2^{n-i} + 2^n deg\ f_i\right) \sigma_{ij}, \end{aligned} \tag{33}$$

wobei für $i \in \mathcal{N}$ gilt: mit $f_i \in \mathbb{F}_p[x_0]$ sind die Nenner von α_i in der Darstellung (30) bezeichnet, und es gilt $\sigma_{ij} := \begin{cases} 1, & \alpha_i \mid w_j \\ 0, & \text{sonst} \end{cases}$.

Da $v_{P_\infty^{(n)}}(w_j) \equiv \sum_{i=1}^{n} \left(-2^{n-i}\right) \sigma_{ij}\ mod\ m$ und $\sum_{i \in V_{j_1}} 2^i \neq \sum_{i \in V_{j_2}} 2^i$ für $V_{j_1} \neq V_{j_2}$ (nach (31) definiert) gilt, folgt

$$v_{P_\infty^{(n)}}(w_i) \not\equiv v_{P_\infty^{(n)}}(w_j)\ mod\ m \text{ für } i \neq j,\ i, j = 1, \ldots, m.$$

Daher bilden $w_1, \ldots, w_m \in F_n$ eine Basis für F_n/F_0.

Lemma 4.2.1 *Sei $n \geq 1$. Für die oben definierte Basis $\{w_1, \ldots, w_m\}$ für F_n/F_0 gilt:*

$$\mathcal{O}_n \subseteq \sum_{i=1}^{m} \mathcal{O}_0 w_i.$$

Beweis. Wir fixieren ein $i \in \mathcal{N}$. Da $F_i = F_{i-1}(x_i)$ und $[F_i : F_{i-1}] = 2$, ist $\{1, \beta_i\}$ eine Basis für F_i/F_{i-1}.

BEHAUPTUNG. $\left\{\frac{1}{2}, \frac{\alpha_i}{2}\right\}$ ist die duale Basis zu $\{1, \beta_i\}$ für F_i/F_{i-1}.
BEWEIS. Sei f_i der Nenner von α_i in der Darstellung (30). Dann ist das Minimalpolynom von β_i: $\varphi(T) = T^2 - \frac{2f_i^2 x_{i-1}}{x_{i-1}^2+1} \in F_{i-1}[T]$. Da $\varphi(\beta_i) = 0$, gilt $\varphi(T) = (T-\beta_i)(T+\beta_i)$ wegen $\beta_i^2 = \frac{2f_i^2 x_{i-1}}{x_{i-1}^2+1}$. Es gilt $\varphi'(\beta_i) = 2\beta_i$. Nach dem Beweis von Theorem III.5.10 [Sti] ist $\left\{\frac{1}{2\beta_i}, \frac{\beta_i}{2\beta_i}\right\} = \left\{\frac{1}{2}, \frac{\alpha_i}{2}\right\}$ die duale Basis zur Basis $\{1, \beta_i\}$ für F_i/F_{i-1}. $\lhd$

Nach Lemma 4.1.3 folgt $v_{P^{(n)}}(\beta_i) \geq 0$ für alle $P^{(n)} \in \mathcal{S}_n$. Daher ist $\beta_i \in \mathcal{O}_n$. Da $\beta_i \in F_i$ und $\mathcal{O}_i = F_i \cap \mathcal{O}_n$, gilt $\beta_i \in \mathcal{O}_i$. So ist $\{1, \beta_i\}$ eine Basis für F_i/F_{i-1} mit Elementen aus $\mathcal{O}_i$. Da $\mathcal{O}_i = ic_{F_i}(\mathcal{O}_{i-1})$, folgt nach der Behauptung und Theorem 2.2.13(2):

$$\mathcal{O}_i \subseteq \frac{1}{2}\mathcal{O}_{i-1} + \frac{\alpha_i}{2}\mathcal{O}_{i-1}.$$

Da $\frac{1}{2} \in \mathbb{F}_p$ ist, gilt

$$\mathcal{O}_i \subseteq \mathcal{O}_{i-1} + \alpha_i\mathcal{O}_{i-1}.$$

Da diese Inklusion für alle $i = 1, \ldots, n$ gilt, folgt:

$$\begin{aligned}
\mathcal{O}_n &\subseteq \mathcal{O}_{n-1} + \alpha_n\mathcal{O}_{n-1} \\
&\subseteq \mathcal{O}_{n-2} + \alpha_{n-1}\mathcal{O}_{n-2} + \alpha_n\mathcal{O}_{n-2} + \alpha_n\alpha_{n-1}\mathcal{O}_{n-2} \\
&\subseteq \ldots \\
&\subseteq \sum_{i=1}^{m} \mathcal{O}_0 w_i.
\end{aligned}$$

□

4.3 Die Zahl Q nach Punkt (4) in Abschnitt 3.1

Seien $w_1, \ldots, w_m$ und $\mathcal{N}$ wie in Abschnitt 4.2 gegeben.

Lemma 4.3.1 *Für jede Zahl $Q \in \mathbb{N}$ mit*

$$Q > \begin{cases} 2^{n-2} + 2^{2n-3}, & n \geq 2 \\ 1, & n = 1 \end{cases}$$

gilt

$$v_{P^{(n)}}(w_i) > -Q$$

für alle $P^{(n)} \in \mathcal{S}_n$ und für $i = 1, \ldots, m$.

Beweis. Wir fixieren den Index $j' \in \{1, \ldots, m\}$, für den gilt

$$w_{j'} = \prod_{i=1}^{n} \alpha_i.$$

Wegen $\beta_i = \frac{1}{\alpha_i} \in \mathcal{O}_n$ folgt $v_{P^{(n)}}(\alpha_i) \leq 0$ für alle $P^{(n)} \in \mathcal{S}_n$ und für $i \in \mathcal{N}$. Damit gilt für alle $P^{(n)} \in \mathcal{S}_n$ und für $j = 1, \ldots, m$:

$$v_{P^{(n)}}(w_{j'}) = \sum_{i=1}^{n} v_{P^{(n)}}(\alpha_i) \leq \sum_{i \in V_j} v_{P^{(n)}}(\alpha_j) = v_{P^{(n)}}(w_j).$$

Wählen wir eine Zahl $Q \in \mathbb{N}$ so, dass

$$v_{P^{(n)}}(w_{j'}) > -Q \tag{34}$$

für alle $P^{(n)} \in \mathcal{S}_n$ gilt, folgt dann

$$v_{P^{(n)}}(w_j) > -Q$$

für alle $P^{(n)} \in \mathcal{S}_n$ und für $j = 1, \ldots, m$. Um eine Zahl Q zu wählen, so dass (34) erfüllt ist, schätzen wir $min\left\{v_{P^{(n)}}\left(\prod_{j=1}^{n}\alpha_j\right) \mid P^{(n)} \in \mathcal{S}_n\right\}$ ab.

Sei $P^{(n)} \in \mathcal{S}_n$. Nach Lemma 4.1.3 gilt:

$$\begin{array}{rcll} v_{P^{(n)}}(\alpha_1) & \geq & -2^{n-1} & \text{für } n \geq 1, \\ v_{P^{(n)}}(\alpha_2) & \geq & -2^{n-2} & \text{für } n \geq 2. \end{array}$$

Damit sind die Fälle für $n = 1, 2$ beschrieben.[11]

Sei $n \geq 3$. Nach Lemma 4.1.3 gilt für $i = 3, \ldots, n$:

$$v_{P^{(n)}}(x_i) \geq \begin{cases} -2^{n-i}, & -1 \leq s < \frac{n}{2} \\ -2^{2s-i}, & \frac{n}{2} \leq s < n \\ 0, & n \leq s \leq n+3 \end{cases}$$

Da $i \leq n$, gilt

$$-2^{n-i} \geq -2^{n-i} \cdot 2^{n-2} \qquad \text{für } n \geq 3,$$

$$-2^{2s-i} \geq -2^{n-i} \cdot 2^{n-2} \qquad \text{für } \tfrac{n}{2} \leq s < n.$$

Daraus folgt für $i = 3, \ldots, n$

$$v_{P^{(n)}}(x_i) \geq -2^{n-i} \cdot 2^{n-2}.$$

Nach Lemma 4.1.3 gilt

$$v_{P^{(n)}}\left((x_0-1)^{2^{i-2}}\right) = \begin{cases} 2^{i-2} \cdot v_{P^{(n)}}(x_0-1), & \text{falls } P^{(n)} \cap F_0 = P_1 \\ 0, & \text{sonst} \end{cases}$$

$$\leq 2^{i-2} \cdot 2^{n-3}.$$

Nun folgt für $i = 3, \ldots, n$:

$$v_{P^{(n)}}(\alpha_i) \geq -2^{n-i} \cdot 2^{n-2} - 2^{i-2} \cdot 2^{n-3}.$$

Damit haben wir für $w_{j'}$:

$$\begin{array}{rcl} v_{P^{(n)}}(w_{j'}) & = & \displaystyle\sum_{i=1}^{n} v_{P^{(n)}}(\alpha_i) \\ & \geq & \displaystyle -2^{n-1} - 2^{n-2} - \sum_{i=3}^{n}\left(2^{n-3} \cdot 2^{i-2} + 2^{n-2} \cdot 2^{n-i}\right) \\ & = & \displaystyle -2^{n-1} - 2^{n-2} - 2^{n-2}\sum_{i=3}^{n}\left(2^{i-3} + 2^{n-i}\right) \end{array}$$

[11] Es gilt für $n = 2$: $2^{n-1} = 2^{2n-3}$.

$$\begin{aligned} &= -2^{n-1} - 2^{n-2} - 2^{n-2}\left(\sum_{s=0}^{n-3} 2^s + \sum_{s=0}^{n-3} 2^s\right) \\ &= -2^{n-1} - 2^{n-2} - 2^{n-1}\sum_{s=0}^{n-3} 2^s \\ &= -2^{n-1} - 2^{n-2} - 2^{n-1}\left(2^{n-2} - 1\right) \\ &= -2^{n-2} - 2^{2n-3}. \end{aligned}$$

□

4.4 Anwendung von Algorithmus 3.9.1, seine Komplexität und Implementierung in der Programmiersprache von Maple 7

4.4.1 Grundlegende Komplexitätsabschätzungen

Sei $X, Y \subset \mathbb{N}$ und seien $f : X \to \mathbb{R}$ und $h : Y \to \mathbb{R}$. Dann schreiben wir $h \in O(f)$, falls ein $c \geq 0$ und ein $n_0 \in \mathbb{N}$ existieren, so dass für alle $n \geq n_0$ gilt:

$$n \in X \cap Y \text{ und } h(n) \leq cf(n).$$

Wir werden bei der Abschätzung der Komplexität des Algorithmus 3.9.1 zur Berechnung einer Basis des Vektorraums $\mathcal{L}\left(rP_\infty^{(n)}\right)$ (wir betrachten den in Abschnitt 4.1 definierten Turm $\mathcal{F}$ algebraischer Funktionenkörper) annehmen, dass die Operationen "ganze Zahl modulo einer Primzahl", "+", "-", "·", "/", bzw. die Relationen ">", "≥", "<", "≤" zwischen zwei ganzen Zahlen jeweils Zeit $O(1)$ benötigen.

Seien $f(x), g(x) \in \mathbb{F}_p[x]$ als Summen der Potenzen von x mit Koeffizienten aus $\mathbb{F}_p$ dargestellt. Im folgenden bezeichnen wir mit

"$f(x)$ multiplizieren mit $g(x)$"

das Aufschreiben $f(x)g(x)$ formal als Produkt und mit

"ausmultiplizieren von $f(x)g(x)$"

die Berechnung des Produkts $f(x)g(x)$.

Nach [Grä], [Knu 1] und [Knu 2] erfordern die aufgelisteten Operationen folgende angegebene Zeiten:

$$C(Berechnung\ von\ ggT(f(x), g(x))) = O(deg\ f(x) \cdot deg\ g(x))$$

$$C(Berechnung\ von\ f(x) + g(x)) = O(max\{deg\ f(x), deg\ g(x)\})$$

$$C(Ausmultiplizieren\ von\ f(x) \cdot g(x)) = O(deg\ f(x) \cdot deg\ g(x))$$

$$C\left(\begin{array}{c} Berechnung\ des\ Rests\ der \\ Division\ von\ f(x)\ durch\ g(x) \end{array}\right) = O(deg\ g(x) \cdot (deg\ f(x) - deg\ g(x)))$$

Nach [Knu 2] und [Rab] kostet die Faktorisierung von $f(x)$ über $\mathbb{F}_p$ folgende Zeit:

$$C(Faktorisierung\ von\ f(x)) = \begin{cases} O(p \cdot deg^3\ f(x)), \text{ für kleine } p \\ O(p \cdot deg^3\ f(x) \cdot log^3 \deg\ f(x)), \text{ für große } p \end{cases}$$

Da wir aber vorausgesetzt haben, dass die Operation "mod p" Zeit $O(1)$ benötigt, kann p in den Abschätzungen weggelassen werden.

Für die Komplexität der Berechnung des Lösungsraums eines linearen Gleichungssystems mit n Gleichungen benutzen wir die Abschätzung für die Komplexität des Gaußschen Algorithmus für eine $[n \times n]$-Matrix nach [Grä] und [Aho-Hop-Ull]:

$$C\left(\begin{array}{c}\textit{Bestimmung des Lösungsraums eines linearen}\\ \textit{Gleichungssystems mit n Gleichungen}\end{array}\right) = O(n^3).$$

Seien A, B zwei beliebige Mengen mit t Elementen. Dann benötigt nach [Aho-Hop-Ull] und [Knu 3]

- jede der Operationen $A \cup B, A \cap B, A \setminus B$ und die Abfrage $a \in A$ Zeit $O(t)$,
- die Feststellung $A = B$ Zeit $O(t^2)$,
- die Operation $A \dot{\cup} B$ Zeit $O(1)$ unter der Voraussetzung, dass $A \cap B = \emptyset$ bekannt ist.

Die Gesamtkomplexität des Algorithmus 3.9.1 ergibt sich aus den Komplexitäten der Berechnungen in den Schritten 1 - 8. Wir werden in den Abschnitten, in denen jeweils ein Schritt durchgeführt wird, die Algorithmen zu den Berechnungen aus diesem Schritt angeben, ihre Komplexität abschätzen, die Abschätzungen erläutern und eine Implementierung in der Programmiersprache von Maple 7 angeben.

Die Gesamtkomplexität des Algorithmus 3.9.1 zur Berechnung einer Basis von $\mathcal{L}\left(rP_\infty^{(n)}\right)$ wird in Abhängigkeit von der Anzahl der rationalen Stellen von $F_n/\mathbb{F}_{p^2}$ abgeschätzt.

4.4.2 Vorbereitungen zum Programm

In den nächsten Abschnitten wird Algorithmus 3.9.1 in der Programmiersprache von Maple 7 implementiert. Wir zeigen zuerst, dass Algorithmus 3.9.1 über $\mathbb{F}_p$ ablaufen wird, bzw. alle Berechnungen in Maple 7 modulo p stattfinden werden.

Für die in Abschnitt 4.2 gewählte Basis $\{w_1, \ldots, w_m\}$ für F_n/F_0 gilt

$$w_i \in \mathbb{F}_p(x_0, x_1, \ldots, x_n) \text{ für } i = 1, \ldots, m,$$

und die Voraussetzungen von Abschnitt 3.8 sind erfüllt.[12] Daher setzen wir

$$Q := min\{\ p^a \mid a \in \mathbb{N},\ \text{und } p^a \text{ erfüllt Lemma 4.3.1}\}.$$

Damit werden alle Berechnungen in Algorithmus 3.9.1 über $\mathbb{F}_p$ ablaufen.

Input des Programms:

n - der Index, für den wir die Funktionenkörpererweiterung F_n/F_0 betrachten.
p - die Charakteristik des Grundkörpers $\mathbb{F}_{p^2}$, $p \neq 2$.
r - eine nichtnegative ganze Zahl, die den Vektorraum $\mathcal{L}\left(rP_\infty^{(n)}\right)$ bestimmt.

[12] Als L wird der Körper $\mathbb{F}_p(x_0, \ldots, x_n)$ betrachtet, wobei x_0 transzendent über $\mathbb{F}_{p^2}$ ist und jedes x_i die Gleichung (25) (Seite 37) für $i \geq 1$ erfüllt.

Liste aller globalen Variablen:

m - der Grad der Funktionenkörpererweiterung $[F_n : F_0]$, wird in der Prozedur Basis berechnet.

$w||i$ - das Basiselement w_i, definiert nach (32) in Abschnitt 4.2, wird in der Prozedur Basis berechnet.

$infval||i$ - $v_{P_\infty^{(n)}}(w_i)$, wird nach (33) aus Abschnitt 4.2 in der Prozedur Basis berechnet.

Q - p^a, wird nach Lemma 4.3.1 in der Prozedur ZahlQ berechnet.

$W||i$ - die Basisdarstellung von w_i^Q bezüglich $\{w_1, \ldots, w_m\}$, wird in der Prozedur Basisdarstellung berechnet.

$b(i,j)$ - der Koeffizient b_{ij} aus der Basisdarstellung von $w_i^Q = \sum_{j=1}^m b_{ij} w_j$, wird in der Prozedur Basisdarstellung berechnet.

$D||i$ - das Polynom D_i, definiert nach (4) in Abschnitt 3.4, wird in der Prozedur DPolynome berechnet.

$maxdeg$ - $max\{deg(D_1), \ldots, deg(D_m)\}$, wird in der Prozedur DPolynome berechnet.

$T||t$ - die Menge T_t, definiert in Abschnitt 3.7, wird in der Prozedur TMengen berechnet.

$J||t$ - die Indexmenge J_t, definiert in Abschnitt 3.7, wird in der Prozedur TMengen berechnet.

$number$ - die Zahl $\bar{m} - 1$, wird in der Prozedur TMengen nach Abschnitt 3.7 berechnet.

$Test$ - die Aussage, ob die J_t für $t = 1, \ldots, \bar{m}$ paarweise disjunkt sind: $true$ oder $false$.

$tmenge$ - die Menge $T_{t'} \ni w_k$ für ein $k \in \{1, \ldots, m\}$, wird in der Hilfsprozedur TMenge bezüglich der Variablen k berechnet, TMenge wird in der Prozedur Ganzheitsbasis aufgerufen.

$e[i,s]$ - die Unbestimmte $e_{\phi(i,s)}$, definiert nach (8) in Schritt 2.2 in Algorithmus 3.4.6, wird in der Prozedur Ganzheitsbasis berechnet.

$a||i$ - $a_i(e_1, \ldots, e_l, x)$, definiert nach (8) in Schritt 2.2 in Algorithmus 3.4.6, wird in der Prozedur Ganzheitsbasis berechnet.

$A||i$ - $a_i(e_1, \ldots, e_l, x)^Q$, wird nach Schritt 2.2 in Algorithmus 3.4.6 mit der Annahme $e_i^Q = e_i$ für $i = 1, \ldots, l$ in der Prozedur Ganzheitsbasis berechnet.

$u||k$ - das Ganzheitsbasiselement u_k aus den Algorithmen 3.4.6 und 3.5.3, wird in der Hilfsprozedur DefOne berechnet, DefOne wird in den Prozeduren Ganzheitsbasis und VPolordnungen aufgerufen.

$c(i,k)$ - der Koeffizient $c_{(i,k)}$ aus der Basisdarstellung von $u_k = \sum_{i=1}^m c_{(i,k)} w_i$, wird in den Prozeduren Ganzheitsbasis und VPolordnungen berechnet.

$val||k$ - $v_{P_\infty^{(n)}}(u_k)$, wird in der Hilfsprozedur DefOne berechnet, DefOne wird in den Prozeduren Ganzheitsbasis und VPolordnungen aufgerufen.

$mval||k$ - $v_{P_\infty^{(n)}}(u_k)$ $mod\ m$, wird in der Hilfsprozedur DefOne berechnet, DefOne wird in den Prozeduren Ganzheitsbasis und VPolordnungen aufgerufen.

$basis$ - eine Basis des Vektorraums $\mathcal{L}\left(rP_\infty^{(n)}\right)$, wird in der Prozedur LBasis berechnet.

Das Programm für Algorithmus 3.9.1 ist in Prozeduren aufgeteilt, die in der richtigen Reihenfolge aufgerufen werden müssen.

Aufrufreihenfolge der Prozeduren:

BASIS();
ZAHLQ();
BASISDARSTELLUNG();
DPOLYNOME();
TMENGEN();
DISJUNKTTEST();
GANZHEITSBASIS();
VPOLORDNUNGEN();
LBASIS();

Die Beschreibungen dieser Prozeduren werden in den nächsten Abschnitten angegeben.

4.4.3 Berechnung der Basis $\{w_1, \ldots, w_m\}$ für F_n/F_0

Nach Schritt 1 in Algorithmus 3.9.1 berechnen wir die nach (32) definierte Basis $\{w_1, \ldots, w_m\}$ für F_n/F_0 und nach (33) die Bewertungen $v_{P_\infty^{(n)}}(w_j)$ für $j = 1, \ldots, m$, wobei $m = 2^n$ ist.

Seien $\alpha_1, \ldots, \alpha_n$ mit der Darstellung (30) und $\alpha_0 := 1$ gegeben. Dann können wir die Menge $\{V_j \subseteq \{1, \ldots, n\} \mid V_j$ ist nach (31) definiert, $j = 1, \ldots, m\}$ in Zeit $O(m)$ konstruieren. Nach (32) berechnen wir

$$\left.\begin{array}{l} \text{for } j = 1, \ldots, m \\ \quad w_j = \prod_{i \in V_j} \alpha_i \ mod\ p \ \text{ (Multiplikation)} \\ \text{end for} \end{array}\right\} \text{ in Zeit } O(mn)$$

und nach (33)

$$\left.\begin{array}{l} \text{for } j = 1, \ldots, m \\ \quad v_{P_\infty^{(n)}}(w_j) = 2^n deg_{x_0}(denominator(w_j)) \\ \quad \text{for } i = 1, \ldots, n \\ \quad\quad v_{P_\infty^{(n)}}(w_j) = v_{P_\infty^{(n)}}(w_j) - 2^{n-i} deg_{x_i}(numerator(w_j)) \\ \quad \text{end for} \\ \text{end for} \end{array}\right\} \text{ in Zeit } O(mn^2)$$

Damit ist

$$\boxed{C(Berechnung\ der\ Basis\ \{w_1, \ldots, w_m\}\ für\ F_n/F_0) = O\left(2^n n^2\right).}$$

Die Berechnung von w_j und $v_{P_\infty^n}(w_j)$ für $j = 1, \ldots, m$ findet mittels der Prozedur BASIS statt. Außerdem werden in der Prozedur BASIS die Elemente $w_1, \ldots, w_m$ mittels der Hilfsprozedur SORT sortiert und neu indiziert, so dass gilt:

$$v_{P_\infty^{(n)}}(w_1) > v_{P_\infty^{(n)}}(w_2) > \ldots > v_{P_\infty^{(n)}}(w_m).^{13} \tag{35}$$

Diese Reihenfolge von $w_1, \ldots, w_m$ benötigen wir in Abschnitt 4.4.5.

[13] Da $v_{P_\infty^{(n)}}(w_i) \not\equiv v_{P_\infty^{(n)}}(w_j)\ mod\ m$ für $i \neq j$ (siehe Abschnitt 4.2), gilt immer die "echt größer als" Beziehung.

```
BASIS := proc()
    local i, j, alpha, sorted, powerset;
    global m, w, infval;
    alpha||0 := 1;
    alpha||1 := x||1/(x||0^2 + 1);
    if n > 1 then
        alpha||2 := x||2/(x||0 + 1);
        if n > 2 then
            for i from 3 to n do
                alpha||i := x||i/(x||0 + (p - 1))^(2^(i - 2));
            end do;
        end if;
    end if;
    with(combinat, choose);
    powerset := choose([seq(alpha||i, i = 1..n)]);
    m := nops(powerset);
    for i from 1 to m do
        w||i := product(powerset[i][j], j = 1..nops(powerset[i]));
    end do;
    for j from 1 to m do
        infval||j := 2^n*degree(1/w||j, x||0);
        for i from 1 to n do
            infval||j := infval||j - 2^(n - i)*degree(w||j, x||i);
        end do;
    end do;
    sorted := Sort([seq(infval||i, i = 1..m)], [seq(w||i, i = 1..m)]);
    for i from 1 to m do
        infval||i := sorted[1][i];
        w||i := sorted[2][i];
    end do;
end proc;
```

Die Hilfsprozedur Sort hat als Input zwei gleichlange Listen. Die erste Liste enthält nichtnegative[14] ganze Zahlen (in unserem Fall – $[infval_1, \ldots, infval_m]$), die absteigend sortiert werden sollen. Dabei ändert sich die Reihenfolge der Elemente der zweiten Liste (in unserem Fall ist die zweite Liste – $[w_1, \ldots, w_m]$) entsprechend der Sortierung der Elemente der ersten Liste. Als Output bekommen wir zwei umgeordnete Listen, und es gilt für diese Implementierung:

$$\boxed{C(\textit{Sortierung von } w_1, \ldots, w_m) = O(2^{2n}).}$$

```
SORT := proc(LPol, LBas)
    local i, j, index, Liste, resultp, resultb;
    Liste := LPol;
    resultp := [ ];
    resultb := [ ];
    for i from 1 to nops(Liste) do
        index := 1;
        for j from 2 to nops(Liste) do
```

[14] Folgt aus (33), Seite 42.

```
            if Liste[j] > Liste[index] then
                index := j;
            end if;
        end do;
        resultp := [op(resultp), LPol[index]];
        resultb := [op(resultb), LBas[index]];
        Liste[index] := -1;
    end do;
    return [resultp, resultb];
end proc;
```

Damit ändert sich die gesamte Komplexität von Schritt 1 zu $O(2^{2n})$.

Es existieren nach [Knu 3] und [Aho-Hop-Ull] effizientere Sortierungsalgorithmen, da aber, wie wir später sehen werden, die Gesamtkomplexität des Algorithmus 3.9.1 höher als mit $O(m^2)$ abgeschätzt wird, ist die vorhandene Implementierung ausreichend.

Bemerkung 4.4.3.1 *Da* $1 \in \{w_1, \ldots, w_m\}$*, folgt* $w_m = 1$ *nach dem Ablauf der Prozedur* BASIS*. Damit gilt:*
1. $w_m^Q = 1 \Longrightarrow V_m = \emptyset$.[15]
2. $w_i^Q = \sum_{j=1}^{m-1} b_{ij} w_j$ *für* $i = 1, \ldots, m-1$ *(folgt aus Konstruktion (32) von* $w_1, \ldots, w_m$ *aus Abschnitt 4.2, und da* $Q \equiv 1 \bmod 2$ *ist.)*

Aus den Punkten 1 und 2 folgt unmittelbar:
3. $D_m = 1$.
4. $T_{\bar{m}} = \{1\}$*, und* $J_{\bar{m}} = \{m\}$.
5. $J_{\bar{m}} \bigcap J_t = \emptyset$ *für* $t < \bar{m}$.
6. $u_m = 1$*, und* $v_{P_\infty^{(n)}}(u_m) = 0$.

4.4.4 Berechnung der Zahl $Q = p^a$

Nach Schritt 2 in Algorithmus 3.9.1 berechnen wir die kleinste natürliche Zahl Q, so dass $Q = p^a$ für ein $a \in \mathbb{N}$, und Q erfüllt Lemma 4.3.1. Wir betrachten die Berechnung von Q für $n \geq 2$:

$a = 1$
$bound = 2^{2n-3} + 2^{n-2}$
while $p^a \leq bound$
    $a = a + 1$
end while
$Q = p^a$

Die "while"-Schleife läuft, solange $p^a \leq 2^{2n-3} + 2^{n-2} < 2^{2n}$ erfüllt ist. Damit ist die letzte Potenz a, die noch berechnet wird, kleiner als $2n$, unter der Voraussetzung $p > 2$.

Damit ist

$$\boxed{C(Berechnung\ der\ Zahl\ Q) = O\left(n^2\right).}$$

```
ZAHLQ := proc()
    local a, bound;
```

[15] Definiert in (31), Seite 42.

```
    global Q;
    a := 1;
    if n >= 2 then
        bound := 2^(2*n - 3) + 2^(n - 2);
        while p^a <= bound do
            a := a + 1;
        end do;
    end if;
    Q := p^a;
end proc;
```

4.4.5 Berechnung der Basisdarstellungen von $w_1^Q, \ldots, w_m^Q$

Nach Schritt 3 in Algorithmus 3.9.1 müssen wir die Basisdarstellungen von w_i^Q in F_n/F_0 für $i = 1, \ldots, m$ berechnen:

$$w_i^Q = \sum_{j=1}^{m} b_{ij} w_j, \tag{36}$$

wobei $b_{ij} \in \mathbb{F}_p(x_0)$ für $i, j = 1, \ldots, m$. Nach Bemerkung 4.4.3.1(1) und (36) folgt, dass jedes w_i^Q für $i = 1, \ldots, m-1$ als ein Quotient darstellbar ist, in dem

- der Zähler ein Polynom aus $\mathbb{F}_p[x_0, x_1, \ldots, x_n]$ ist, in dem die Unbestimmten $x_1, \ldots, x_n$ jeweils höchstens in der ersten Potenz auftreten.
- der Nenner ein Polynom aus $\mathbb{F}_p[x_0]$ ist.

(37)

Da die Nenner von $w_1^Q, \ldots, w_{m-1}^Q$ wegen (32) (Seite 42) sowieso Polynome aus $\mathbb{F}_p[x_0]$ sind, genügt es, eine Darstellung nach (37) für $\prod_{i\in V_j} x_i^Q$, wobei V_j nach (31) (Seite 42) definiert ist, für $j = 1, \ldots, m-1$ zu bestimmen. Dafür werden wir einen Algorithmus angeben, der die drei folgenden Substitutionen für $i \geq 1$ anwendet:

$$x_i^2 = \frac{x_{i-1}^2 + 1}{2x_{i-1}} \tag{38}$$

$$x_i + 1 = \frac{(x_{i-1} - 1)^2}{2x_{i-1}(x_i - 1)} \tag{39}$$

$$x_i - 1 = \frac{(x_{i-1} - 1)^2}{2x_{i-1}(x_i + 1)} \tag{40}$$

Die erste ist die den Turm definierende Gleichung (25) aus Abschnitt 4.1, und die beiden anderen ergeben sich aus (38).

Algorithmus 4.4.5.1 *Eine Darstellung nach (37) für $\prod_{i\in V_j} x_i^t$ für ein $t \in \mathbb{N}$ und für ein $j \in \{1, \ldots, m-1\}$.*

Input: $E = \prod_{i\in V_j} x_i^t$

for $i = n, \ldots, 1$

$E = (substitution\ (38) \to E)\ mod\ p$
if $x_i \mid denominator(E)$
$E = (substitution\ (38) \to x_i * numerator(E))\ /\ (substitution\ (38) \to x_i * denominator(E))\ \ mod\ p$
end if
if $i > 1$
while $x_{i-1} + 1 \mid denominator(E)$
$E = numerator(E)\ /\ (substitution\ (39)\ mod\ p\ \to denominator(E))\ mod\ p$
end while
while $(x_{i-1} - 1)\ mod\ p \mid denominator(E)$
$E = numerator(E)\ /\ (substitution\ (40)\ mod\ p\ \to denominator(E))\ mod\ p$
end while
end if
end do

Output: E in der Darstellung (37)

Lemma 4.4.5.2 *Mit Algorithmus 4.4.5.1 wird eine Darstellung nach (37) für* $\prod_{i \in V_j} x_i^t$ *für* $j = 1, \ldots, m-1$ *und für alle* $t \in \mathbb{N}$ *bestimmt.*

Beweis. Da die Schleife nach i von n bis 1 abwärts läuft, werden durch die Substitution (38) alle Potenzen von x_i größer als 1 durch Ausdrücke in der Unbestimmten x_{i-1}, eventuell mit der ersten Potenz von x_i multipliziert, sukzessive ersetzt. Damit folgt unmittelbar aus der Struktur des Algorithmus, dass der Zähler von E beim Output die Darstellung (37) hat. Wir müssen noch zeigen, dass mittels dieses Algorithmus der Nenner von E beim Output ein Polynom aus $\mathbb{F}_p[x_0]$ ist.

Zuerst stellen wir folgendes fest: wenn wir zeigen, dass der Algorithmus für x_i^t für alle $t \in \mathbb{N}$ und für $i = 1, \ldots, n$ funktioniert, gilt dies auch für $\prod_{i \in V_j} x_i^t$ für alle $t \in \mathbb{N}$ und für $j = 1, \ldots, m-1$. Wegen (38) und da für $t \geq 3$ jedes $x_i^t = (x_i^2)^v * x_i^\sigma$ mit $v \in \mathbb{N}$ und $\sigma \in \{0, 1\}$ gilt, folgt, dass es genügt, die Korrektheit des Algorithmus für x_i^2 zu zeigen.

Sei $i \in \{1, \ldots, n\}$. Nun starten wir mit x_i^2. Wir lassen die Berechnungen von den Koeffizienten der Unbestimmten $x_0, x_1, \ldots, x_n$ weg und benutzen deswegen das Zeichen "=". Wir führen die Berechnungen nur in den entstehenden Nennern durch, d.h. wir lassen zuerst alle Polynome aus $\mathbb{F}_p[x_0, \ldots, x_{i-1}]$ in den entstehenden Zählern unverändert. Damit gilt:

$$x_i^2 \quad \text{“}= \text{“} \quad \frac{x_{i-1}^2 + 1}{x_{i-1}}$$

$$(38) \to x_{i-1} * Nenner$$

$$\text{“}= \text{“} \quad \frac{(x_{i-1}^2 + 1) x_{i-1} x_{i-2}}{x_{i-2}^2 + 1}$$

$$(38) \to Nenner$$

$$\text{“}=\text{“}\quad \frac{(x_{i-1}^2+1)x_{i-1}x_{i-2}x_{i-3}}{(x_{i-3}+1)^2}$$

$$(39)\ mod\ p\ \rightarrow Nenner$$

$$\text{“}=\text{“}\quad \frac{(x_{i-1}^2+1)x_{i-1}x_{i-2}x_{i-3}x_{i-4}^2(x_{i-3}+(p-1))^2}{(x_{i-4}+(p-1))^{2^2}}$$

$$(40)\ mod\ p\ \rightarrow Nenner$$

$$\text{“}=\text{“}\quad \frac{(x_{i-1}^2+1)x_{i-1}x_{i-2}x_{i-3}x_{i-4}^2x_{i-5}^{2^2}(x_{i-3}+(p-1))^2(x_{i-4}+1)^{2^2}}{(x_{i-5}+(p-1))^{2^3}}$$

$$(40)\ mod\ p\ \rightarrow Nenner$$

$$\text{“}=\text{“}\quad \ldots$$

$$(40)\ mod\ p\ \rightarrow Nenner$$

$$\text{“}=\text{“}\quad \frac{(x_{i-1}^2+1)x_{i-1}x_{i-2}(x_{i-3}+(p-1))^2\prod_{l=0}^{i-3}x_l^{2^{i-3-l}}\prod_{l=1}^{i-4}(x_l+1)^{2^{i-2-l}}}{(x_0+(p-1))^{2^{i-2}}}.$$

Da wir für die höheren Potenzen von $x_1,\ldots,x_{i-1}$ im Zähler das gleiche Verfahren wie für x_i^2 rekursiv anwenden können, folgt, dass der Algorithmus beim Output x_i^2 in der Darstellung (37) liefert.

□

Nun berechnen wir die Komplexität des Algorithmus 4.4.5.1 beim Input

$$E=\prod_{i=1}^{n}x_i^Q,$$

da es sich theoretisch um den schlechtesten Fall handelt. Wir lassen die Operation “mod p“ aus unseren Betrachtungen weg, da sie nach der Voraussetzung Zeit $O(1)$ benötigt. Da die Schleife nach i in Algorithmus 4.4.5.1 von n bis 1 abwärts läuft, werden wir über den “k-ten Schleifendurchlauf“ im Fall $i=k$ reden, d.h., dass der Algorithmus mit dem n-ten Schleifendurchlauf beginnt.

Sei $k\in\{1,\ldots,n\}$. Wir listen alle Berechnungen auf, die im k-ten Schleifendurchlauf stattfinden können:

1) in der Zeile “$E=substitution\ (38)\rightarrow E$“

i) in dieser Reihenfolge im Zähler von E:
- das Ausmultiplizieren der Faktoren und die Addition von Koeffizienten bei gleichen Potenzen von x_k

$$f_\gamma x_k^\gamma+f_{\gamma-1}x_k^{\gamma-1}+\cdots+f_0,$$

wobei $\gamma\in\mathbb{N}$, und für $j=0,\ldots,\gamma$ gilt: $f_j\in\mathbb{F}_p[x_0,\ldots,x_n]\backslash\{\mathbb{F}_p[x_k]\backslash\mathbb{F}_p\}$, so dass, falls $k\leq n-1$, gilt: $deg_{x_l}f_j\leq 1$ für $l=k+1,\ldots,n$. (Aufgrund des Verlaufs

des Algorithmus 4.4.5.1 mit dem Input $E = \prod_{i=1}^{n} x_i^Q$.)
- die Durchführung von (38) in den Potenzen von x_k, (kein Ausmultiplizieren der dadurch entstandenen Potenzen von $x_{k-1}^2 + 1$ notwendig!)

$$x_k^{\gamma \bmod 2} \left(\frac{x_{k-1}^2+1}{2x_{k-1}}\right)^{\lfloor \frac{\gamma}{2} \rfloor} f_\gamma + x_k^{\gamma-1 \bmod 2} \left(\frac{x_{k-1}^2+1}{2x_{k-1}}\right)^{\lfloor \frac{\gamma-1}{2} \rfloor} f_{\gamma-1} + \cdots + f_0.$$

- die Berechnung eines gemeinsamen Nenners, bzw. die Darstellung des Zählers von E als Quotient zweier Polynome

$$\frac{x_k^{\gamma \bmod 2} \left(x_{k-1}^2+1\right)^{\lfloor \frac{\gamma}{2} \rfloor} f_\gamma + x_k^{\gamma-1 \bmod 2} \left(x_{k-1}^2+1\right)^{\lfloor \frac{\gamma-1}{2} \rfloor} (2x_{k-1}) f_{\gamma-1} + \cdots + f_0 (2x_{k-1})^{\lfloor \frac{\gamma}{2} \rfloor}}{(2x_{k-1})^{\lfloor \frac{\gamma}{2} \rfloor}}.$$

ii) im Nenner[16] von E

$$x_k^{\eta_1} (x_k^2+1)^{\eta_2} (x_{k-1} + (p-1))^{\eta_3}$$

mit $\eta_j \in \mathbb{N} \cup \{0\}$ für $j = 1, 2, 3$ die Durchführung von (38) (kein Ausmultiplizieren der Faktoren notwendig!)

$$x_k^{\eta_1 \bmod 2} \left(\frac{x_{k-1}^2+1}{2x_{k-1}}\right)^{\lfloor \frac{\eta_1}{2} \rfloor} \left(\frac{x_{k-1}^2+1}{2x_{k-1}} + 1\right)^{\eta_2} (x_{k-1} + (p-1))^{\eta_3}.$$

iii) die Darstellung von E als Quotient zweier Polynome

$$E = \frac{\left(x_k^{\gamma \bmod 2} (x_{k-1}^2+1)^{\lfloor \frac{\gamma}{2} \rfloor} f_\gamma + \cdots + f_0 (2x_{k-1})^{\lfloor \frac{\gamma}{2} \rfloor}\right) (2x_{k-1})^{\lfloor \frac{\eta_1}{2} \rfloor + \eta_2}}{(2x_{k-1})^{\lfloor \frac{\gamma}{2} \rfloor} x_k^{\eta_1 \bmod 2} (x_{k-1}^2+1)^{\lfloor \frac{\eta_1}{2} \rfloor} (x_{k-1}+1)^{2\eta_2} (x_{k-1} + (p-1))^{\eta_3}}.$$

2) in dem "if"-Block (Schleifendurchlauf für $i = k$)

i) die Abfrage

"if $x_i \mid denominator(E)$".

Dies ist der Fall, wenn $\eta_1 \equiv 1 \ mod\ 2$. Gelte dieser Fall weiter.
ii) in der Zeile

"$E = subs.\ (38) \to x_i * numerator(E)\ /\ subs.\ (38) \to x_i * denominator(E)$"

- die Division des Nenners von E durch x_k und die Multiplikation mit der rechten Seite der Gleichung (38) (kein Ausmultiplizieren notwendig!)

$$(2x_{k-1})^{\lfloor \frac{\gamma}{2} \rfloor - 1} (x_{k-1}^2+1)^{\lfloor \frac{\eta_1}{2} \rfloor + 1} (x_{k-1}+1)^{2\eta_2} (x_{k-1} + (p-1))^{\eta_3}.$$

- das Ausmultiplizieren des Zählers von E (der Zähler selbst muß nicht zuerst als Summe von Monomen dargestellt werden) mit x_k, zum Beispiel für $\gamma \equiv 1 \ mod\ 2$

$$\Big(x_k^2 (x_{k-1}^2+1)^{\lfloor \frac{\gamma}{2} \rfloor} f_\gamma + \cdots + x_k^2 (x_{k-1}^2+1)^{\lfloor \frac{\gamma-2}{2} \rfloor} f_{\gamma-2} (2x_{k-1})^2 + \ \cdots \\ + \ f_0 (2x_{k-1})^{\lfloor \frac{\gamma}{2} \rfloor}\Big) (2x_{k-1})^{\lfloor \frac{\eta_1}{2} \rfloor + \eta_2}.$$

[16] Die angegebene Darstellung hat der Nenner von E unmittelbar vor dem k-ten Schleifendurchlauf aufgrund des Verlaufs des Algorithmus.

- die Durchführung von (38) in den (gegebenenfalls) dadurch entstandenen x_k^2 im Zähler von E

$$\left(\frac{x_{k-1}^2+1}{2x_{k-1}}(x_{k-1}^2+1)^{\lfloor\frac{\gamma}{2}\rfloor}f_\gamma+\cdots+f_0\,(2x_{k-1})^{\lfloor\frac{\gamma}{2}\rfloor}\right)(2x_{k-1})^{\lfloor\frac{\eta_1}{2}\rfloor+\eta_2}.$$

- die Darstellung von E als Quotient zweier Polynome

$$\frac{(x_{k-1}^2+1)^{\lfloor\frac{\gamma}{2}\rfloor+1}(2x_{k-1})^{\lfloor\frac{\eta_1}{2}\rfloor+\eta_2}f_\gamma+\cdots+f_0(2x_{k-1})^{\lfloor\frac{\gamma}{2}\rfloor+\lfloor\frac{\eta_1}{2}\rfloor+\eta_2+1}}{(2x_{k-1})^{\lfloor\frac{\gamma}{2}\rfloor}(x_{k-1}^2+1)^{\lfloor\frac{\eta_1}{2}\rfloor+1}(x_{k-1}+1)^{2\eta_2}(x_{k-1}+(p-1))^{\eta_3}}.$$

3) in den beiden "while"-Schleifen endlich oft (Schleifendurchlauf für $i=k$)

i) die Überprüfung

"while $x_{i-1}+1 \mid denominator(E)$, "

bzw.

"while $x_{i-1}+(p-1) \mid denominator(E)$".

ii) in der Zeile

$$E = numerator(E)\ /\ (substitution\ (39) \rightarrow denominator(E))$$

- die Division des Nenners von E durch $x_{k-1}+1$, bzw. durch $x_{k-1}+(p-1)$, und die Multiplikation (kein Ausmultiplizieren) mit der rechten Seite von (39), bzw. von (40) (für $k-1$)

$$\frac{(2x_{k-2})^{2\eta_2+\eta_3}(x_{k-1}+(p-1))^{2\eta_2}(x_{k-1}+1)^{\eta_3}\left((x_{k-1}^2+1)^{\lfloor\frac{\gamma}{2}\rfloor+1}(2x_{k-1})^{\lfloor\frac{\eta_1}{2}\rfloor+\eta_2}f_\gamma+\cdots\right)}{(2x_{k-1})^{\lfloor\frac{\gamma}{2}\rfloor}(x_{k-1}^2+1)^{\lfloor\frac{\eta_1}{2}\rfloor+1}(x_{k-2}+(p-1))^{2(2\eta_2+\eta_3)}}.$$

Für die Berechnung der Komplexität der Punkte 1)-3) führen wir andere Potenzbezeichnungen ein, durch die diese Komplexität besser ausgedrückt werden kann. Nach dem obigen Verfahren hat E unmittelbar vor dem k-ten Schleifendurchlauf folgende Darstellung:[17]

$$E = x_1^Q\cdots x_k^Q\frac{x_{k-1}^{\nu_1+\nu_2}(x_k+(p-1))^{\nu_1}(x_k+1)^{\nu_2}f(x_k,x_{k+1},\ldots,x_n)}{x_k^{\mu_1}(x_k^2+1)^{\mu_2}(x_{k-1}+(p-1))^{2\nu_1+2\nu_2}} \qquad (41)$$

mit

$$f(x_k,x_{k+1},\ldots,x_n)=\sum_{2\xi_1+\xi_2\leq\chi}g_{(\xi_1,\xi_2)}(x_{k+1},\ldots,x_n)(x_k^2+1)^{\xi_1}x_k^{\xi_2},$$

wobei $\chi = deg_{x_k}f(x_k,x_{k+1},\ldots,x_n)$, $\nu_l,\mu_l,\xi_l\in\mathbb{N}\cup\{0\}$ für $l=1,2$, das Polynom $g_{(\xi_1,\xi_2)}(x_{k+1},\ldots,x_n)$ ist ausmultipliziert, und es gilt für $j=k+1,\ldots,n$: $deg_{x_j}g_{(\xi_1,\xi_2)}(x_{k+1},\ldots,x_n)\leq 1$.

[17] Wir betrachten den k-ten Schleifendurchlauf für ein $k\leq n-1$, da im n-ten Schleifendurchlauf mit dem Input $E=\prod_{i=1}^n x_i^Q$ nicht mehr Berechnungen als in einem späteren Schleifendurchlauf stattfinden.

Als erstes muß der Zähler von E in der Darstellung (41) ausmultipliziert werden. Da es sich um Ausmultiplizieren der binomischen Formel handelt, wird das Ausmultiplizieren der Potenzen ν_1, ν_2 und ξ_1 auf die Berechnung von binomialen Koeffizienten reduziert. Die Komplexität für ihre Berechnung ist mit $C\left(\textit{Berechnung von } \begin{pmatrix} n \\ l \end{pmatrix}\right) = O(l)$ abgeschätzt. Damit erfordert das Ausmultiplizieren von $(x_k + (p-1))^{\nu_1}$ Zeit, die nicht schlechter als $O(\nu_1^2)$ ist, das Ausmultiplizieren von $(x_k + 1)^{\nu_2}$ Zeit, die nicht schlechter als $O(\nu_2^2)$ ist, das Ausmultiplizieren von allen Summanden in der Summe $\sum_{2\xi_1+\xi_2\leq\chi} \dots$ Zeit, die nicht schlechter ist als

$$O\left(2^{n-k}\chi^4\right).^{18} \tag{42}$$

Nach der Addition (ihre Rechenzeit ist in der vorherigen Rechenzeit enthalten) der Koeffizienten bei den gleichen Potenzen von x_k in der ausmultiplizierten Summe $\sum_{2\xi_1+\xi_2\leq\chi} \dots$ wird das endgültige Ausmultiplizieren im Zähler von E

$$x_1^Q \cdots x_k^Q x_{k-1}^{\nu_1+\nu_2}(x_k^{\nu_1} + \cdots)(x_k^{\nu_2} + \cdots) \sum_{l=0}^{\chi} h_l(x_{k+1}, \dots, x_n) x_k^l$$

ausgeführt, wobei $deg_{x_j} h_l(x_{k+1}, \dots, x_n) \leq 1$, $l = 0, \dots, \chi$ und $j = k+1, \dots, n$. Dies benötigt Zeit

$$O(2^{n-k}\nu_1\nu_2\chi).$$

Danach folgt die Addition (ihre Rechenzeit ist in der vorherigen Rechenzeit enthalten) der Koeffizienten bei gleichen Potenzen von x_k. Die Durchführung von (38) benötigt Zeit

$$O\left((Q + \nu_1 + \nu_2 + \chi)^2\right),$$

da sie in jeder Potenz von x_k (nicht größer als $Q + \nu_1 + \nu_2 + \chi$) je maximal $(Q + \nu_1 + \nu_2 + \chi)/2$ mal durchführbar ist.

Aus der Beschreibung der Punkte 1)-3) folgt, dass die weiteren Berechnungen (im k-ten Schleifendurchlauf) Zeit erfordern, die nicht schlechter ist als die oben angegebene.[19]

Daher müssen nur ν_1, ν_2 und χ abgeschätzt werden.

Definition 4.4.5.3 *Der* **Grad eines multivariablen Polynoms**

$$F = \sum_{(\tau_0,\dots,\tau_n)\in(\mathbb{N}\cup\{0\})^n} \left(\Upsilon(\tau_0, \dots, \tau_n) \prod_{i=0}^{n} x_i^{\tau_i}\right) \in \mathbb{F}_p[x_0, \dots, x_n],$$

wobei alle $\Upsilon(\tau_0, \dots, \tau_n) \in \mathbb{F}_p$ *sind, ist wie folgt definiert:*

$$deg\ F := max\left\{\sum_{i=0}^{n} \tau_i \mid \Upsilon(\tau_0, \dots, \tau_n) \neq 0\right\}.$$

[18] Die Anzahl der Summanden in der Summe $\sum_{2\xi_1+\xi_2\leq\chi} \dots$ ist nicht größer als χ^2. Das Ausmultiplizieren eines der Summanden $g_{(\xi_1,\xi_2)}(x_{k+1}, \dots, x_n)(x_k^2 + 1)^{\xi_1} x_k^{\xi_2}$ benötigt Zeit, die nicht schlechter als $O(2^{n-k}\chi^2)$ ist, da die Anzahl der verschiedenen Summanden in $g_{(\xi_1,\xi_2)}(x_{k+1}, \dots, x_n)$ nicht größer als $2^{n-k} + 1$ ist.

[19] Dazu müssen wir nur Punkt 1) ii) genauer diskutieren. Die Komplexität dieser Berechnungen ist $O(\mu_1)$. Da wir für die Abschätzung der Gesamtkomplexität nicht berücksichtigen, dass Kürzungen im Zähler und im Nenner möglich sind oder, dass die Summe einiger Koeffizienten zu 0 in $\mathbb{F}_p$ werden kann, sondern vom schlechtesten Fall ausgehen, folgt, dass sich der Term $(x_k^2 + 1)^{\mu_1}$ wegen (38) im Zähler befindet. Somit ist $O(\mu_1)$ bereits in der oben angegebenen Komplexität enthalten.

Da $Q+\nu_1+\nu_2+\chi$ nicht größer als der Grad des Zählers von E in der Darstellung (41) ist, benötigen die Berechnungen im gesamten k-ten Schleifendurchlauf Zeit nicht schlechter als

$$O\left(2^{n-k}\cdot(\textit{Grad des Zählers von } E \textit{ in } (41))^4\right). \tag{43}$$

Wir bezeichnen für $k=1,\ldots,n$ mit dem angegebenen Namen den Grad des folgenden multivariablen Polynoms:

$Z_k^{(0)}$ – des Zählers von E unmittelbar vor dem k-ten Schleifendurchlauf,
$N_k^{(0)}$ – des Nenners von E unmittelbar vor dem k-ten Schleifendurchlauf,
$Z_k^{(1)}$ – des Zählers von E unmittelbar vor dem Ablauf des "if"-Blocks im k-ten Schleifendurchlauf,
$N_k^{(1)}$ – des Nenners von E unmittelbar vor dem Ablauf des "if"-Blocks im k-ten Schleifendurchlauf,
$Z_k^{(2)}$ – des Zählers von E unmittelbar vor dem Ablauf der beiden "while"-Schleifen im k-ten Schleifendurchlauf,
$N_k^{(2)}$ – des Nenners von E unmittelbar vor dem Ablauf der beiden "while"-Schleifen im k-ten Schleifendurchlauf,
$Z_0^{(0)}$ – des Zählers von E beim Output,
$N_0^{(0)}$ – des Nenners von E beim Output.

Lemma 4.4.5.4 *Für $k=1,\ldots,n$ gilt:*

$$\begin{aligned}
Z_{k-1}^{(0)} &\leq Z_k^{(2)}+2N_k^{(2)},\\
N_{k-1}^{(0)} &\leq 2N_k^{(2)},\\
Z_k^{(1)} &\leq Z_k^{(0)}+\frac{1}{2}max\left\{Z_k^{(0)},N_k^{(0)}\right\},\\
N_k^{(1)} &\leq max\left\{Z_k^{(0)},N_k^{(0)}\right\},\\
Z_k^{(2)} &\leq Z_k^{(1)}+2,\\
N_k^{(2)} &\leq N_k^{(1)}+1.
\end{aligned}$$

Beweis. Wir beweisen zuerst die dritte und die vierte Abschätzung. Für $k=n$ gilt:

$$Z_n^{(0)}=nQ \text{ und } N_n^{(0)}=0.$$

Vor dem "if"-Block wird die Substitution (38) im Zähler von E durchgeführt. Aufgrund ihrer Darstellung folgt:

$$Z_n^{(1)}=Z_n^{(0)} \text{ und } N_n^{(1)}\leq\frac{1}{2}Z_n^{(0)}. \tag{44}$$

Sei $k\in\{1,\ldots,n-1\}$. Dann gilt unmittelbar vor dem k-ten Schleifendurchlauf

$$E=\frac{x_k^{\gamma}f_\gamma+x_k^{\gamma-1}f_{\gamma-1}+\cdots+x_kf_1+f_0}{x_k^{\eta_1}(x_k^2+1)^{\eta_2}g(x_{k-1})},$$

wobei $\gamma,\eta_1,\eta_2\in\mathbb{N}\cup\{0\}$, $f_j\in\mathbb{F}_p[x_0,\ldots,x_{k-1},x_{k+1},\ldots,x_n]$ für $j=0,\ldots,\gamma$, $Z_k^{(0)}=max\{deg\ f_j+j\mid j=0,\ldots,\gamma\}$ und $\eta_1+2\eta_2+deg\ g(x_{k-1})=N_k^{(0)}$. Nach

der Durchführung von (38) sieht E dann wie folgt aus:

$$\begin{aligned} E &= \frac{x_k^{\gamma \bmod 2}\left(\frac{x_{k-1}^2+1}{2x_{k-1}}\right)^{\lfloor\frac{\gamma}{2}\rfloor} f_\gamma + x_k^{\gamma-1 \bmod 2}\left(\frac{x_{k-1}^2+1}{2x_{k-1}}\right)^{\lfloor\frac{\gamma-1}{2}\rfloor} f_{\gamma-1} + \cdots + f_0}{x_k^{\eta_1 \bmod 2}\left(\frac{x_{k-1}^2+1}{2x_{k-1}}\right)^{\lfloor\frac{\eta_1}{2}\rfloor}\left(\frac{x_{k-1}^2+1}{2x_{k-1}}+1\right)^{\eta_2} g(x_{k-1})} \\ &= \frac{\left(x_k^{\gamma \bmod 2}(x_{k-1}^2+1)^{\lfloor\frac{\gamma}{2}\rfloor} f_\gamma + \cdots + f_0(2x_{k-1})^{\lfloor\frac{\gamma}{2}\rfloor}\right)(2x_{k-1})^{\lfloor\frac{\eta_1}{2}\rfloor+\eta_2}}{x_k^{\eta_1 \bmod 2}(x_{k-1}^2+1)^{\lfloor\frac{\eta_1}{2}\rfloor}(x_{k-1}+1)^{2\eta_2} g(x_{k-1})(2x_{k-1})^{\lfloor\frac{\gamma}{2}\rfloor}}. \end{aligned}$$

Der Grad des Zählers von E wächst am meisten im Fall $deg\ f_0 = \gamma = Z_k^{(0)}$ und $\eta_1 + 2\eta_2 = N_k^{(0)}$, und der Grad des Nenners von E wächst am meisten im Fall $\gamma = Z_k^{(0)}$. Unabhängig von der bestehenden "kleiner-gleich"-Relation zwischen γ und $\eta_1 + 2\eta_2$ gilt:

$$Z_k^{(1)} \leq Z_k^{(0)} + \frac{1}{2} max\left\{Z_k^{(0)}, N_k^{(0)}\right\}$$

und

$$N_k^{(1)} \leq max\left\{Z_k^{(0)}, N_k^{(0)}\right\}.$$

Wir beweisen die vier weiteren Abschätzungen. Sei $k \in \{1, \ldots, n\}$.

Die Berechnungen im "if"-Block werden nur im Fall durchgeführt, falls x_k (nicht eine seiner Potenzen!) ein Faktor des Nenners von E ist. Da (38) für höhere Potenzen von x_k schon durchgeführt wurde, hat E vor dem "if"-Block die Darstellung:

$$E = \frac{g_1 + g_2 x_k}{g_3 x_k},$$

wobei $g_j \in \mathbb{F}_p[x_0, \ldots, x_n] \setminus \{\mathbb{F}_p[x_k] \setminus \mathbb{F}_p\}$ für $j = 1, 2, 3$, $N_k^{(1)} = deg\ g_3 + 1$ und $Z_k^{(1)} = max\{deg\ g_1, deg\ g_2 + 1\}$. Der "if"-Block wird dann wie folgt durchgeführt:

$$E = \frac{g_1 x_k + g_2 x_k^2}{g_3 x_k^2} = \frac{g_1 x_k + g_2 \frac{x_{k-1}^2+1}{2x_{k-1}}}{g_3 \frac{x_{k-1}^2+1}{2x_{k-1}}} = \frac{2g_1 x_k x_{k-1} + g_2(x_{k-1}^2+1)}{g_3(x_{k-1}^2+1)}.$$

Da der Fall $deg\ g_1 = Z_k^{(1)}$ auftreten kann, gilt:

$$Z_k^{(2)} \leq Z_k^{(1)} + 2$$

und

$$N_k^{(2)} \leq N_k^{(1)} + 1.$$

Der Grad des Zählers und der Grad des Nenners von E wachsen während der Durchläufe der "while"-Schleifen am meisten, falls der Nenner nur aus Potenzen von $x_{k-1} + 1$ und (oder) von $x_{k-1} + (p-1)$ besteht. Dann sieht

$$E = \frac{f}{(x_{k-1} + (p-1))^{\theta_1}(x_{k-1}+1)^{\theta_2}},$$

wobei $\theta_j \in \mathbb{N} \cup \{0\}$ für $j = 1, 2$, $f \in \mathbb{F}_p[x_0, \ldots, x_n]$, $N_k^{(2)} = \theta_1 + \theta_2$ und $Z_k^{(2)} = deg\ f$, nach der Durchführung von (39) und (40) wie folgt aus:

$$E = \frac{f(2x_{k-2}(x_{k-1}+1))^{\theta_1}(2x_{k-2}(x_{k-1}+(p-1)))^{\theta_2}}{(x_{k-2}+(p-1))^{2\theta_1+2\theta_2}}.$$

Damit folgt:

$$Z_{k-1}^{(0)} \leq Z_k^{(2)} + 2N_k^{(2)}$$

und

$$N_{k-1}^{(0)} \leq 2N_k^{(2)}.$$

□

Lemma 4.4.5.5 *Für $k = 0, \ldots, n-1$ gilt:*

$$max\left\{Z_k^{(0)}, N_k^{(0)}\right\} \leq 4^{n-k+1}nQ.$$

Beweis. Nach Lemma 4.4.5.4 gilt:

$$\begin{aligned}
Z_k^{(0)} &\leq Z_{k+1}^{(2)} + 2N_{k+1}^{(2)} \\
&\leq Z_{k+1}^{(1)} + 2N_{k+1}^{(1)} + 4 \\
&\leq Z_{k+1}^{(0)} + \frac{5}{2}max\left\{Z_{k+1}^{(0)}, N_{k+1}^{(0)}\right\} + 4 \\
&\leq \frac{7}{2}\left(Z_{k+2}^{(2)} + 2N_{k+2}^{(2)}\right) + 4 \qquad \text{vergleiche mit der ersten Zeile} \\
&\leq \left(\frac{7}{2}\right)^2\left(Z_{k+3}^{(2)} + 2N_{k+3}^{(2)}\right) + 4 + 4\cdot\frac{7}{2} \\
&\leq \left(\frac{7}{2}\right)^{n-k-1}\left(Z_n^{(2)} + 2N_n^{(2)}\right) + 4\left(1 + \frac{7}{2} + \cdots + \left(\frac{7}{2}\right)^{n-k-2}\right) \\
&\leq \left(\frac{7}{2}\right)^{n-k-1}\left(Z_n^{(1)} + 2N_n^{(1)}\right) + 4\left(1 + \frac{7}{2} + \cdots + \left(\frac{7}{2}\right)^{n-k-1}\right) \\
&\leq \left(\frac{7}{2}\right)^{n-k-1}\left(\frac{3}{2}Z_n^{(0)}\right) + 4\cdot\left(\frac{7}{2}\right)^{n-k} \quad \text{nach (44)} \\
&\leq \left(\frac{7}{2}\right)^{n-k}\left(\frac{3}{7}Z_n^{(0)} + 4\right) \\
&\leq 4^{n-k+1}nQ,
\end{aligned}$$

$$\begin{aligned}
N_k^{(0)} &\leq 2N_{k+1}^{(2)} \\
&\leq Z_{k+1}^{(2)} + 2N_{k+1}^{(2)} \\
&\leq 4^{n-k+1}nQ, \qquad \text{analog zu } Z_k^{(0)}.
\end{aligned}$$

□

Nach (43) (Seite 57), Lemma 4.4.5.5, und da insgesamt n Schleifendurchläufe stattfinden, folgt:

$$\begin{aligned} C\left(\textit{Alg. } 4.4.5.1 \textit{ mit dem Input } \prod_{i=1}^{n} x_i^Q\right) &= O\left(n \cdot 2^{n-1}\left(4^n nQ\right)^4\right) \\ &= O\left(2^{9n} n^5 Q^4\right). \end{aligned}$$

Der Algorithmus 4.4.5.1 wird in der Prozedur ERSATZ implementiert. Die Substitution (38) wird mit dem Maple 7 Befehl "algsubs" durchgeführt, die Substitutionen (39) - (40) jedoch nicht, da der Output des Befehls "algsubs" in diesem Fall nicht das gewünschte Ergebnis liefert.[20]

```
ERSATZ := proc(expression)
    local i, j1, j2, N, Z, E, Rest;
    E := expression mod p;
    for i from n by (-1) to 1 do
        E := (algsubs((x||i)^2 = (x||(i - 1)^2 + 1)/(2*x||(i - 1)), Expand(numer(E))
        mod p)) / (algsubs((x||i)^2 = (x||(i - 1)^2 + 1)/(2*x||(i - 1)),
        denom(E) mod p)) mod p;
        N := denom(E);
        if divide(N, x||i, 'Rest') = true then
            N := Rest*((x||(i - 1))^2+1);
            Z := numer(E)*2*(x||(i - 1))*x||i mod p;
            Z := (algsubs((x||i)^2 = (x||(i - 1)^2 + 1)/(2*x||(i - 1)),
            Expand(Z) mod p) mod p;
        else
            Z := numer(E);
        end if;
        if i >1 then
            j1 := 0;
            while Divide(N, x||(i - 1) + 1, 'Rest') mod p = true do
                j1 := j1 + 1;
                N := Rest mod p;
            end do;
            j2 := 0;
            while Divide(N, x||(i - 1) - 1, 'Rest') mod p = true do
                j2 := j2 + 1;
                N := Rest mod p;
            end do;
            Z := Z*(2*x||(i - 2)*(x||(i - 1) + (p - 1))/(x||(i - 2) + (p - 1))^2)^(j1)
            *(2*x||(i - 2)*(x||(i - 1) + 1)/ (x||(i - 2) + (p - 1))^2)^(j2) mod p;
        end if;
        E := Z/N mod p;
    end do;
    return E;
end proc;
```

[20] Zum Beispiel gibt $algsubs(x+1=a,(x+1)x)$ als Output $a(a-1)$. Solche Effekte wollen wir aber vermeiden.

Nach dem Ablauf des Algorithmus 4.4.5.1 gilt für $i = 1, \ldots, m-1$ [21]

$$w_i^Q = \frac{\sum_{j=1}^{m-1} \sum_{k\geq 0} \gamma_{ijk} x_0^k \prod_{t\in V_j} x_t}{h_i(x_0)}, \tag{45}$$

wobei $h_i(x_0) \in \mathbb{F}_p[x_0]$, und $\gamma_{ijk} \in \mathbb{F}_p$ für $i, j = 1, \ldots, m-1$ und für $k \geq 0$.

Der nächste Algorithmus schreibt w_i^Q für $i = 1, \ldots, m-1$ in der Darstellung

$$w_i^Q = \sum_{j=1}^{m-1} b_{ij} \text{`}w\text{`}_j$$

durch Symbole $\text{`}w\text{`}_1, \ldots, \text{`}w\text{`}_{m-1}$ auf. Wir werden im weiteren die folgende Substitution für $j = 1, \ldots, m-1$ anwenden:

$$\prod_{i\in V_j} x_i = \text{`}w_j\text{`} \cdot denominator(w_j), \tag{46}$$

wobei $denominator(w_j)$ nach der Darstellung (32) (Seite 42) definiert ist. Dann gilt (Erklärungen zu den Komplexitätsabschätzungen sind weiter unten):

for $i = 1, \ldots, m-1$
  $w_i^Q = Alg.4.4.5.1 \rightarrow numerator(w_i^Q)$ / $denominator(w_i^Q)$ } in Zeit $O\left(2^{9n} n^5 Q^4\right)$
  $Z = numerator(w_i^Q)$
  for $j = 1, \ldots, m-1$
    $Z = substitution(46) \rightarrow Z \bmod p$ } in Zeit $O(2^{3n} nQ)$
  end for
  for $j = 1, \ldots, m-1$
    $b_{ij} = simplify\left(coefficient_{\text{`}w_j\text{`}}(Z)/denominator(w_i^Q)\right)$ } in Zeit $O\left(2^{7n} n^3 Q^3\right)$
  end for
  $w_i^Q = \sum_{i=1}^{m-1} b_{ij} \text{`}w\text{`}_j$
end for

Wegen der Sortierung (35) (Seite 48) gilt: bei der sukzessiven Durchführung von (46) wird das Produkt $\prod_{i\in V_{j_1}} x_i$ nie vor dem Produkt $\prod_{i\in V_{j_2}} x_i$ ersetzt für alle $V_{j_1} \subsetneqq V_{j_2}$.[22] Dies garantiert uns die Korrektheit des Algorithmus, bzw. die Korrektheit der Basisdarstellungen von $w_1^Q, \ldots, w_{m-1}^Q$.

Aus (45) folgt, dass die Substitution (46) in jedem Schleifendurchlauf der inneren "for"-Schleife Zeit $O(deg_{x_0} Z)$ erfordet. Da $deg_{x_0} Z \leq Z_0^{(0)}$, gilt nach Lemma 4.4.5.5 die Abschätzung $O(4^n nQ)$.

Für $i, j = 1, \ldots, m-1$ gilt: der Grad des Zählers von b_{ij} ist nicht größer als $Z_0^{(0)}$, der Grad des Nenners[23] von b_{ij} ist nicht größer als $N_0^{(0)} + (2^{n-1}+1)Q$. Um zu erreichen, dass der Zähler und der Nenner von b_{ij} teilerfremd sind, können

[21] Siehe auch Bemerkung 4.4.3.1(1),(2).

[22] V_j ist in (31), Seite 42, definiert. Durch die Sortierung (35) garantieren wir folgendes: sei zum Beispiel $a_1 = x_1x_2$, $a_2 = x_3x_4$ $a_3 = x_1x_2x_3x_4$. Nach unserem Vorgehen wird das Produkt $\prod_{i=1}^4 x_i$ durch a_3 und nicht durch a_1a_2 ersetzt.

[23] Die Nenner mit den höchsten Graden haben theoretisch gesehen b_{1j} für $j = 1, \ldots, m-1$, da der Nenner von w_1^Q (nach (35), Seite 48, gilt $w_1 = \prod_{i=1}^n \alpha_i$, siehe auch (30), Seite 42)

wir, zum Beispiel, durch ihre Faktorisierungen über $\mathbb{F}_p$ die gleichen Faktoren kürzen, wobei wir im weiteren feststellen werden, dass die Faktorisierungen die Gesamtkomplexität des Algorithmus 3.9.1 nicht vergrößern!

Die Faktorisierungen in b_{ij} kosten für kleine p Zeit

$$O\left(\left(Z_0^{(0)}\right)^3 + \left(N_0^{(0)} + (2^{n-1}+1)Q\right)^3\right)$$

und für große p Zeit

$$O\left(\left(Z_0^{(0)}\right)^3 \cdot log^3\left(Z_0^{(0)}\right) + \left(N_0^{(0)} + (2^{n-1}+1)Q\right)^3 \cdot log^3\left(N_0^{(0)} + (2^{n-1}+1)Q\right)\right).$$

Nach Lemma 4.4.5.5 gilt:

$$O\left((4^n nQ)^3\right) \text{ für kleine } p$$

und

$$O\left((4^n nQ)^3 log^3\left(4^n nQ\right)\right) \text{ für große } p.$$

Wir betrachten die kleinen p. Da die Außenschleife $m-1$ mal läuft, gilt:

$$\boxed{\begin{array}{rcl} C\left(\textit{Basisdarstellungen von } w_1^Q, \ldots, w_m^Q\right) & = & O\left(m\ 2^{9n} n^5 Q^4\right) \\ & = & O\left(2^{10n} n^5 Q^4\right). \end{array}}$$

```
BASISDARSTELLUNG := proc()
    local i, j, Z;
    global b, W;
    for i from 1 to m - 1 do
        W||i := Ersatz(numer(w||i)^Q)/denom(w||i)^Q mod p;
        Z := numer(W||i) mod p;
        for j from 1 to m - 1 do
            Z := algsubs(numer(w||j) = denom(w||j)*'w'||j, Expand(Z) mod p)
            mod p;
        end do;
        for j from 1 to m - 1 do
            b(i, j) := simplify((Factor(coeff(Z, 'w'||j)) mod p)/
            (Factor(denom(W||i)) mod p)) mod p;
        end do;
        W||i := sum('b(i, j)*'w'||j', 'j' = 1..m - 1);
    end do;
    W||m := 1;
end proc;
```

beim Input gleich $h(x_0) := \left((x_0^2+1)(x_0+1)\prod_{i=3}^{n}(x_0+(p-1))^{2^{i-2}}\right)^Q$ ist, und damit den größten Grad hat. Nach dem Ablauf von Algorithmus 4.4.5.1 ändert sich der ursprüngliche Nenner von w_1^Q zu $h_1(x_0) = f(x_0)h(x_0)$, wobei $f(x_0) \in \mathbb{F}_p[x_0]$ mit $deg\ f(x_0) \leq N_0^{(0)}$. Dadurch können die Grade der Nenner von allen b_{ij} abgeschätzt werden.

4.4.6 Berechnung der Polynome $D_1, \ldots, D_m$

Nach Schritt 4 in Algorithmus 3.9.1 berechnen wir Polynome $D_1, \ldots, D_m$. In Abschnitt 4.4.5 in der Prozedur Basisdarstellung sind alle $b_{ij} \in \mathbb{F}_p(x_0)$ berechnet worden, und ihre Nenner[24] d_{ij} sind dabei über $\mathbb{F}_p$ faktorisiert worden. Aus Algorithmus 4.4.5.1 folgt, dass für $i, j = 1, \ldots, m-1$ gilt:

$$d_{ij} = x_0^{\mu_{ij}}(x_0^2+1)^{\nu_{ij}}(x_0+1)^{\eta_{ij}}(x_0+(p-1))^{\xi_{ij}}{}^{25} \tag{47}$$

für gewisse $\mu_{ij}, \nu_{ij}, \eta_{ij}, \xi_{ij} \in \mathbb{N} \cup \{0\}$. Wir implementieren die Berechnung der Polynome $D_1, \ldots, D_m$ unter Berücksichtigung von Bemerkung 4.4.3.1(3) genau nach dem Verfahren in Abschnitt 3.4.

for $i = 1, \ldots, m-1$
  $d_i = kgV(d_{i1}, \ldots, d_{im-1})$
  $d_i = \prod_{s=1}^{t_i} f_{si}^{g_{si}}$ (Faktorisierung)
  for $s = 1, \ldots, t_i$
    $l_{si} = \lceil g_{si}/Q \rceil$
  end for
  $D_i = \prod_{i=1}^{t_i} f_{si}^{l_{si}}$ (Multiplikation)
end for

Aufgrund der Kenntnis der Faktorisierungen von allen d_{ij} können die Berechnung und die Faktorisierung von d_i für $i = 1, \ldots, m-1$ durch einen Vergleich für $j = 1, \ldots, m-1$ der Potenzen gleicher Faktoren in d_{ij} (wird im weiteren genauer erläutert) ausgeführt werden. Dieses Verfahren hat eine niedrigere Komplexität als die Standardverfahren zur Berechnung des kleinsten gemeinsamen Vielfachen oder zur Faktorisierung eines Polynoms. Mit (47) werden die folgenden Werte

$$\begin{aligned} g_{1i} &= max\{\mu_{ij} \mid j = 1, \ldots, m-1\}, \\ g_{2i} &= max\{\nu_{ij} \mid j = 1, \ldots, m-1\}, \\ g_{3i} &= max\{\eta_{ij} \mid j = 1, \ldots, m-1\}, \\ g_{4i} &= max\{\xi_{ij} \mid j = 1, \ldots, m-1\} \end{aligned}$$

für $i = 1, \ldots, m-1$ berechnet. Dies kostet nach [Knu 1] Zeit $O(m)$. Damit werden $d_i = x_0^{g_{1i}}(x_0^2+1)^{g_{2i}}(x_0+1)^{g_{3i}}(x_0+(p-1))^{g_{4i}}$ für $i = 1, \ldots, m-1$ in Zeit $O(m)$ berechnet und gleich als Produkt der Potenzen seiner über $\mathbb{F}_p$ irreduziblen (mit Berücksichtigung der Darstellung von x_0^2+1) Faktoren dargestellt. $D_1, \ldots, D_{m-1}$ werden als Produkt (kein Ausmultiplizieren!) dieser Polynome in den Potenzen l_{si} für $s = 1, \ldots, 4$ dargestellt. Damit ist

$$\boxed{C(Berechnung\ von\ D_1, \ldots, D_m) = O(2^{2n}).}$$

Die Berechnung von $D_1, \ldots, D_{m-1}$ findet mittels der Prozedur DPolynome statt.[26] Außerdem wird $max\{deg(D_1), \ldots, deg(D_{m-1})\}$ (auch in Zeit $O(m)$) berechnet. Dieser Wert wird in der Prozedur Ganzheitsbasis gebraucht. Wir benutzen bei der Implementierung der Prozedur DPolynome den Maple 7 Befehl

[24] Siehe die Darstellung (3), Seite 16.

[25] Wir werden das Polynom x_0^2+1 weiter nur in dieser Darstellung angeben, obwohl es beim Faktorisieren über $\mathbb{F}_p$ in $(x_0+I)(x_0-I)$ zerfallen kann, falls ein $I \in \mathbb{F}_p$ existiert, so dass $I^2 = -1$ ist.

[26] In der Implementierung verwenden wir die Maple 7 Befehle zur Berechnung und zur Faktorisierung von d_i (nicht das obige Verfahren), da die Praxis zeigt, dass die Prozedur DPolynome sehr wenig Rechenzeit im Vergleich zur Gesamtlaufzeit des Programms benötigt.

"Factors mod p". Der Output dieses Befehls zum Beispiel für $f(x) \in \mathbb{F}_p[x]$ mit der Darstellung $\alpha \prod_{i=1}^{r} f_i(x)^{n_i}$ ist $[\alpha, [[f_1(x), n_1], [f_2(x), n_2], \ldots, [f_r(x), n_r]]]$. So können jeder Faktor von $f(x)$ und sein Grad in $f(x)$ mit dem Maple 7 Befehl "op" aus dieser Struktur abgelesen werden.

```
DPolynome := proc()
    local i, j, s, g, f, l, d, fanzahl, F;
    global D, maxdeg;
    for i from 1 to m - 1 do
        for j from 1 to m - 1 do
            d(i, j) := denom(b(i, j));
        end do;
    end do;
    for i from 1 to m - 1 do
        d||i := Factors(lcm(seq(d(i, j), j = 1..m - 1))) mod p;
        fanzahl||i := nops(op(2, d||i));
        for s from 1 to fanzahl||i do
            f(s, i) := op(1, op(s, op(2, d||i)));
            g(s, i) := op(2, op(s, op(2, d||i)));
            l(s, i) := ceil(g(s, i)/Q);
            F(s, i) := f(s, i)^l(s, i);
        end do;
        D||i := product('F(s, i)', 's' = 1..fanzahl||i);
    end do;
    D||m = 1;
    maxdeg: = max(seq(deg(D||i), i = 1..m - 1));
end proc;
```

4.4.7 Berechnung der Mengen $T_1, \ldots, T_{\bar{m}}$ und ein Disjunktionstest für die Indexmengen $J_1, \ldots, J_{\bar{m}}$

Nach Schritt 5 in Algorihmus 3.9.1 und unter Berücksichtigung von Bemerkung 4.4.3.1(4) berechnen wir die Mengen $T_1, \ldots, T_{\bar{m}}$, in die die Basiselemente $w_1, \ldots, w_m$ nach dem Verfahren in Abschnitt 3.7 disjunkt unterteilt werden, und die Indexmengen $J_1, \ldots, J_{\bar{m}}$. Die Berechnung von T_t und J_t für $t = 1, \ldots, \bar{m}-1$ wird wie folgt ausgeführt:

```
for i = 1, ..., m - 1                    }
    B_i = ∅                              }
    for j = 1, ..., m - 1                }
        if b_ij ≠ 0                      } in Zeit O(m^2)
            B_i = B_i ∪ {j}              }
        end if                           }
    end for                              }
end for                                  }
I = {1, ..., m - 1}
t = 0
```

```
while |I| > 0
    t = t + 1
    Index = das erste Element in I
    T_t = {w_Index}
    J_t = B_Index
    Ĩ_t = {Index}
    for alle i ∈ I \ Ĩ_t
        if B_Index = B_i
            T_t = T_t ∪ {w_i}
            Ĩ_t = Ĩ_t ∪ {i}
        end if
    end for
    I = I \ Ĩ_t
end while
```

Der größte Aufwand entsteht im Fall $B_i = B_j$ für $i, j = 1, \ldots, m$. Dann läuft die "while"-Schleife einmal, die "for"-Schleife $m-2$ mal, und die Berechnungen in der Zeile "if $B_{Index} = B_i$" erfordern Zeit $O(m^2)$. Damit gilt:

$$\boxed{C(\textit{Berechnung von } T_1, \ldots, T_{\bar{m}} \textit{ und } J_1, \ldots, J_{\bar{m}}) = O(2^{3n}).}$$

TMengen := proc()

```
local i, j, t, B, Iset, Isubset, Index;
global number, T, J;
B := array(1..m - 1);
for i from 1 to m - 1 do
    B[i] := {};
    for j from 1 to m - 1 do
        if b(i, j) <> 0 then
            B[i] := B[i] union {j};
        end if;
    end do;
end do;
Iset := {seq(i, i = 1..m - 1)};
t := 0;
while nops(Iset) > 0 do
    t := t + 1;
    Index := Iset[1];
    T||t := {w||Index};
    J||t := B[Index];
    Isubset := {Index};
    for i in (Iset minus Isubset) do
        if B[Index] = B[i] then
            T||t := T||t union {w||i};
            Isubset := Isubset union {i};
        end if;
    end do;
    Iset := Iset minus Isubset ;
end do;
number := t;
```

```
    T||(number + 1) := {1};
    J||(number + 1) := {m};
end proc;
```

Unter Berücksichtigung von Bemerkung 4.4.3.1(5) wird ein Disjunktionstest für die Mengen J_t für $t = 1, \ldots, \bar{m} - 1$ in der Prozedur DISJUNKTTEST wie folgt durchgeführt

```
DISJUNKTTEST := proc()
    local i, j;
    global Test;
    i := 1;
    Test := true;
    while (Test = true) and (i < number) do
        j := i + 1;
        while (Test = true) and (j <= number) do
            if (J||i intersect J||j) <> { } then
                Test := false;
            end if;
            j := j + 1;
        end do;
        i := i + 1;
    end do;
end proc;
```

und kostet Zeit

$$\boxed{C(Disjunktionstest\ für\ J_1, \ldots, J_{\bar{m}-1}) = O(2^{2n}).}$$

Ist der Output von DISJUNKTTEST "true", so bedeutet dies, dass die Indexmengen J_t für $t = 1, \ldots, \bar{m}$ paarweise disjunkt sind, und dass Proposition 3.7.1 angewendet werden kann.

4.4.8 Berechnung einer Ganzheitsbasis für F_n/F_0

Nach Schritt 6 in Algorithmus 3.9.1 wird eine Ganzheitsbasis $\{u_1, \ldots, u_m\}$ für F_n/F_0 berechnet. Wir verfolgen Algorithmus 3.4.6. Nach Schritt 1 gilt für $k = 1$

$$c_{(1,1)} = D_1 \text{ und } u_1 = D_1 w_1,$$

und nach Bemerkung 4.4.3.1(6) gilt für $k = m$

$$u_m = 1.$$

Daher betrachten wir Schritt 2 für ein $k \in \{2, \ldots, m-1\}$. Ist das Ergebnis vom Disjunktionstest "true", stellen wir zuerst fest, in welcher Menge $T_{t'}$ für ein $t' \in \{1, \ldots, \bar{m}\}$ das Element w_k liegt. Dies wird unter Berücksichtigung von Bemerkung 4.4.3.1(5) wie folgt durchgeführt:

$t' = 1$
while $member(w_k, T_{t'}) = false$
    $t' = t' + 1$
end while
$tmenge = T_{t'}$

Die Abfrage $member(w_k, T_{t'})$ erfordet Zeit $O(m)$, und die "while"-Schleife läuft höchstens $\bar{m} \leq m$ mal. Dann gilt:

$$C\left(Fixierung\ der\ Menge\ T_{t'} \ni w_k\right) = O\left(2^{2n}\right).$$

Dieses Verfahren ist in der Hilfsprozedur TMENGE implementiert, und die Menge $T_{t'} \ni w_k$ wird in *tmenge* gespeichert.[27] Damit können wir in der Prozedur GANZHEITSBASIS testen, ob $w_i \in T_{t'}$ für $i \neq k$ ist: $member(w||i, tmenge)$.

```
TMENGE := proc(wk)
    local t;
    global tmenge;
    t := 1;
    while member(wk, T||t) = false do
        t := t + 1;
    end do;
    tmenge := T||t;
end proc;
```

Wir führen jetzt einige Vorbereitungen durch. Seien $i, j = 1, \ldots, m$. Dann gilt für $b_{ij} = \frac{b'_{ij}}{d_{ij}}$ aus den Basisdarstellungen von $w_i^Q = \sum_{j=1}^{m-1} b_{ij} w_j$ folgendes:[28]

$$\begin{aligned} deg\ b'_{ij} &\leq Z_0^{(0)}, \\ deg\ d_{ij} &\leq N_0^{(0)} + (2^{n-1}+1)Q. \end{aligned} \tag{48}$$

Damit, und da jedes d_{ij} ein Produkt von Potenzen von höchstens vier verschiedenen Polynomen[29] ist, gilt

$$deg\ kgV(d_{i1}, \ldots, d_{im-1}) \leq 4\left(N_0^{(0)} + (2^{n-1}+1)Q\right) \tag{49}$$

und analog

$$deg\ kgV(d_{1j}, \ldots, d_{kj}) \leq 4\left(N_0^{(0)} + (2^{n-1}+1)Q\right). \tag{50}$$

Da $\lceil \frac{s}{Q} \rceil \leq \frac{s}{Q} + 1$ für alle $s \in \mathbb{N}$ gilt, folgt nach (4) (Seite 16) und nach (49)

$$deg\ D_i \leq 4\left(\frac{N_0^{(0)}}{Q} + (2^{n-1}+1)\right) + 4. \tag{51}$$

Damit gilt nach Folgerung 3.4.3

$$deg\ c_{(i,i)} \ \leq \ 4\left(\frac{N_0^{(0)}}{Q} + 2^{n-1} + 2\right). \tag{52}$$

[27] Da *tmenge* nur in der Prozedur GANZHEITSBASIS in der Schleife nach k gebraucht wird und als selbstständiges Ergebnis nicht interessant ist, benötigt sie keine Indizierung.

[28] Siehe Begründung dafür auf Seite 61.

[29] Siehe (47), Seite 63. Falls das Polynom x_0^2+1 zerfällt, haben seine beiden Faktoren immer die gleichen Grade, was aber keinen Unterschied im Vergleich zum irreduziblen x_0^2+1 für die folgenden Abschätzungen macht.

Alle weiter angegebenen Algorithmen (Teile von Algorithmus 3.4.6) sind für ein $k \in \{2, \ldots, m-1\}$ geschrieben unter der Voraussetzung, dass die Berechnungen für $i = 2, \ldots, k-1$ bereits stattgefunden haben.

Sei also $k \in \{2, \ldots, m-1\}$. Dann sind $deg\ c_{(i,i)}$ für $i = 1, \ldots, k-1$ bekannt, und wir können $deg\ a_i(e_1, \ldots, e_l, x)$[30] nach Schritt 2.1, (51) und (52) abschätzen. Nach Schritt 2.2 werden $a_i(e_1, \ldots, e_l, x)$ und $a_i(e_1, \ldots, e_l, x)^Q$ unter Berücksichtigung von Proposition 3.7.1 und $e^Q_{\phi(i,s)} = e_{\phi(i,s)}$[31] für $i = 1, \ldots, k$ wie folgt konstruiert:

$a_k(e_1, \ldots, e_l, x) = \sum_{s=0}^{deg\ D_k} e_{\phi(k,s)} x_0^s$
$a_k(e_1, \ldots, e_l, x)^Q = \sum_{s=0}^{deg\ D_k} e_{\phi(k,s)} x_0^{sQ}$
Fixierung von $T_{t'} \ni w_k$ (mit $O(m^2)$ abgeschätzt)
for $i = 1, \ldots, k-1$
  if $Disjunktionstest = false$ or ($Disjunktionstest = true$ and $member(w_i, T_{t'}) = true$)
    $a_i(e_1, \ldots, e_l, x) = \sum_{s=0}^{deg\ c_{(i,i)}-1} e_{\phi(i,s)} x_0^s$
    $a_i(e_1, \ldots, e_l, x)^Q = \sum_{s=0}^{deg\ c_{(i,i)}-1} e_{\phi(i,s)} x_0^{sQ}$
  else
    $a_i(e_1, \ldots, e_l, x) = 0$
    $a_i(e_1, \ldots, e_l, x)^Q = 0$
  end if
end for

Die Abfrage $member(w_i, T_{t'})$ benötigt Zeit $O(m)$. Die Eingabe der Summen kostet nach (51) und (52) je Zeit $O\left(\frac{N_0^{(0)}}{Q}\right)$. Wegen $k \leq m-1$ gilt dann

$$\begin{aligned} C(Konstruktion\ von\ a_i(e_1, \ldots, e_l, x),\ i = 1, \ldots, k) &= O\left(m\left(m + \frac{N_0^{(0)}}{Q}\right)\right) \\ &\subseteq O\left(2^{3n} n\right). \end{aligned}$$

Damit ist alles vorbereitet, um die Division im Quotienten (10) (Seite 23), den wir hier als $\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b_{ij}$ betrachten werden, durchzuführen und den Lösungsraum des linearen Gleichungssystems (12) (Seite 25) zu bestimmen.

[30] Siehe (8), Seite 22.
[31] $\phi(i,s)$ ist auf Seite 21 definiert.

$LGS1 = \{\}$
for $j = 1, \ldots, m-1$
  $R_j = numerator\left(\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b_{ij}\right)$ /
  $denominator\left(\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b_{ij}\right)$ $mod\ p$

  if $R_j \neq 0$
    for $i = 0, \ldots, deg\ R_j$
      $LGS1 = LGS1 \cup \left\{Koeffizient_{x_0^i} R_j = 0\right\}$
    end for
  end if
end for

Sei $j \in \{1, \ldots, m-1\}$. Die Berechnungen in der Zeile

$$\text{“}R_j = numer.\left(\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b_{ij}\right) \text{ / } denom.\left(\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b_{ij}\right)\text{“}$$

werden in der Reihenfolge

$$\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b_{ij} = \sum_{i=1}^{k} \frac{a_i(e_1, \ldots, e_l, x)^Q b'_{ij}}{d_{ij}} = \frac{\sum_{i=1}^{k} a_i(e_1, \ldots, e_l, x)^Q b'_{ij} h_{ij}}{kgV(d_{1j}, \ldots, d_{kj})},$$

wobei $h_{ij} := \frac{kgV(d_{1j}, \ldots, d_{kj})}{d_{ij}}$ für $i = 1, \ldots, k$, wie folgt ausgeführt:
i) Das Ausmultiplizieren der Faktoren in $b'_{ij} \in \mathbb{F}_p[x_0]$ für $i = 1, \ldots, k$ und die Addition modulo p der Koeffizienten bei gleichen Potenzen von x_0 benötigen analog zu den Überlegungen zu (42) (Seite 56) nach Lemma 4.4.5.5 Zeit

$$O\left(m\left(Z_0^{(0)}\right)^4\right) \subseteq O\left(m\left(4^n nQ\right)^4\right).$$

ii) Das Ausmultiplizieren von $a_i(e_1, \ldots, e_l, x)^Q b'_{ij}$ für $i = 1, \ldots, k$ und die Addition der Koeffizienten (enthalten die Unbestimmten $e_1, \ldots, e_l$) bei gleichen Potenzen von x_0 benötigen nach (48), (51), (52) und Lemma 4.4.5.5 Zeit

$$O\left(m\left(Z_0^{(0)}\left(4N_0^{(0)} + 2^{n+1}Q + 7Q\right)\right)\right) \subseteq O\left(m\left(4^n nQ\right)^2\right).$$

iii) Die Berechnung von $kgV(d_{1j}, \ldots, d_{kj})$: aufgrund der Kenntnis der Faktorisierungen von d_{ij} kann sie durch einen Vergleich der Potenzen gleicher Faktoren in d_{ij} für $i = 1, \ldots, k$ durchgeführt werden[32] und benötigt daher Zeit

$$O(m^2) = O(2^{2n}).$$

iv) Das Ausmultiplizieren der Faktoren in $h_{ij} := \frac{kgV(d_{1j}, \ldots, d_{kj})}{d_{ij}}$ für $i = 1, \ldots, k$ und die Addition modulo p der Koeffizienten bei gleichen Potenzen von x_0 wird wie folgt ausgeführt: das Ausmultiplizieren der Potenzen der Faktoren[33] (maximal vier) kann auf die Berechnung der binomialen Koeffizienten reduziert

[32] Analog zu Abschnitt 4.4.6, Seite 63.
[33] Jeder Faktor ist eine binomische Formel.

werden, das Ausmultiplizieren der ausmultiplizierten Potenzen dieser Faktoren benötigt nach (50) (Seite 67) und Lemma 4.4.5.5 Zeit

$$O\left(m\left(N_0^{(0)}+(2^{n-1}+1)Q\right)^4\right)\subseteq O\left(m\left(4^n nQ\right)^4\right).$$

Das Ausmultiplizieren von $kgV(d_{1j},\ldots,d_{kj})$ ist in der angegebenen Komplexität enthalten.
v) Das Ausmultiplizieren von $\left(a_i(e_1,\ldots,e_l,x)^Q b'_{ij}\right)h_{ij}$ für $i=1,\ldots,k$ und die Berechnung von $\sum_{i=1}^k a_i(e_1,\ldots,e_l,x)^Q b'_{ij}h_{ij}$ kostet nach Lemma 4.4.5.5 Zeit

$$O\left(m\left(deg\ b'_{ij}+deg\ a_i(e_1,\ldots,e_l,x)^Q\right)deg\ h_{ij}\right)\subseteq O\left(m\left(4^n nQ\right)^2\right).$$

vi) Die Division von $\sum_{i=1}^k a_i(e_1,\ldots,e_l,x)^Q b'_{ij}h_{ij}$ durch $kgV(d_{1j},\ldots,d_{kj})$ ist in der angegebenen Komplexität enthalten.

Da die Schleife nach j $m-1$ mal läuft, gilt

$$\begin{aligned} C(\textit{Division in } (10) \textit{ in Schritt } 2.2 \textit{ in Alg. } 3.4.6) &= O\left(m^2\left(4^n nQ\right)^4\right)\\ &= O\left(2^{10n}n^4Q^4\right). \end{aligned}$$

Die Anzahl der Gleichungen im linearen Gleichungssystem (12)[34] ist gleich $\sum_{j=1}^{m-1}(deg\ R_j+1)$. Da $deg\ R_j\leq deg\ \left(\sum_{i=1}^k a_i(e_1,\ldots,e_l,x)^Q b'_{ij}h_{ij}\right)$ für $j=1,\ldots,m-1$ gilt, folgt nach Lemma 4.4.5.5:

$$\begin{aligned} C(\textit{Lösung des Systems } (12) \textit{ in Schritt } 2.2 \textit{ in Alg. } 3.4.6) &= O\left(\left(m\ 4^n nQ\right)^3\right)\\ &= O\left(2^{9n}n^3Q^3\right). \end{aligned}$$

Der Divisionsalgorithmus und die Lösung des linearen Gleichungssystems sind in der Hilfsprozedur DivSys implementiert:

```
DivSys := proc(k)
    local eqns, i, j, R, S;
    eqns := {};
    for j from 1 to m - 1 do
        for i from 1 to k do
            S(i, j) := (A||i)*b(i, j);
        end do;
        S||j := sum('S(i, j)', 'i' = 1..k);
        R||j := Rem(numer(S||j), denom(S||j), x||0) mod p;
        if R||j <> 0 then
            for i from 0 to degree(R||j) do
                eqns := eqns union {coeff(R||j, x||0, i) = 0};
            end do;
        end if;
    end do;
    msolve(eqns, p);
end proc;
```

[34] Siehe Seiten 24 - 25.

Nach der Lösung des Systems (12) in Schritt 2.2 können wir $a_i(e_1,\ldots,e_l,x)$ nach (14) in Schritt 2.3 für $i=1,\ldots,k$ darstellen:

for $i=1,\ldots,k-1$
  if $a_i(e_1,\ldots,e_l,x)\neq 0$
    $a_i(\lambda_1,\ldots,\lambda_d,x) = Lösung1 \rightarrow a_i(e_1,\ldots,e_l,x)\ mod\ p$
  end if
end for

Die Anzahl der Unbestimmten, die durch diese Lösung in jedem $a_i(e_1,\ldots,e_l,x)$ ersetzt werden, ist nicht größer als $deg\ c_{(i,i)}$ (siehe (8), Seite 22). Nach (52) (Seite 67) gilt dann:

$$\begin{aligned} C(a_i(e_1,\ldots,e_l,x)\ in\ der\ Darstellung\ (14)\ für\ i=1,\ldots,k) &= O\left(m\frac{N_0^{(0)}}{Q}\right) \\ &= O\left(2^{3n}n\right). \end{aligned}$$

Die Berechnung von $c_{(k,k)} = ggT(a_k(\lambda_1,\ldots,\lambda_d,x),D_k)$ benötigt nach (51), (52) (Seite 67) und Lemma 4.4.5.5 Zeit

$$C\left(Berechnung\ von\ c_{(k,k)}\right) = O\left(\left(4^n n\right)^2\right) = O(2^{4n}n^2).$$

Nach Schritt 2.4 bestimmen wir $c_{(i,k)}$ für $i=1,\ldots,k-1$ wie folgt:

$LGS2 = \{\}$
for $s=0,\ldots,deg\ c_{(k,k)}$
  $LGS2 = \left\{Koeffizient_{x_0^s}a_k(\lambda_1,\ldots,\lambda_d,x) = Koeffizient_{x_0^s}c_{(k,k)}\right\} \cup LGS2$
end for
for $s = deg\ c_{(k,k)}+1,\ldots,deg\ a_k(\lambda_1,\ldots,\lambda_d,x)$
  $LGS2 = \left\{Koeffizient_{x_0^s}a_k(\lambda_1,\ldots,\lambda_d,x)=0\right\} \cup LGS2$
end for
} in Zeit $O\left(2^{2n}n\right)$

$Lösung2 = solve(LGS2, modulo\ p)$ in Zeit $O\left(2^{6n}n^3\right)$

for $i=1,\ldots,k-1$
  if $a_i(\lambda_1,\ldots,\lambda_d,x)\neq 0$
    $c_{(i,k)} = Lösung2 \rightarrow a_i(\lambda_1,\ldots,\lambda_d,x)\ mod\ p$
  else
    $c_{(i,k)} = 0$
  end if
end for
} in Zeit $O(2^{6n}n^2)$

Die Unbestimmten $\lambda_1,\ldots,\lambda_d$ werden durch die Lösung des zweiten Systems in $a_i(\lambda_1,\ldots,\lambda_d,x)$[35] insgesamt nicht mehr als $d(deg\ a_i(\lambda_1,\ldots,\lambda_d,x)+1)$ mal ersetzt, wobei $d<l\leq\sum_{i=1}^k deg\ D_i$ ist.[36] Daher benötigt die dritte "for"-Schleife Zeit $O(m\cdot d\cdot deg\ a_i(\lambda_1,\ldots,\lambda_d,x)) \subseteq O\left(2^{6n}n^2\right)$. Nach Lemma 4.4.5.5 gilt dann

$$C\left(Berechnung\ von\ c_{(i,k)}\ für\ i=1,\ldots,k-1\right) = O\left(2^{6n}n^3\right).$$

[35] In der Darstellung (14), Seite 25.
[36] d und l sind auf den Seiten 20 und 22 definiert.

Da die obigen Berechnungen für jedes $k = 2, \ldots, m-1$ durchgeführt werden, und da alle obigen Abschätzungen für jedes $k = 2, \ldots, m-1$ gelten, folgt

$$\boxed{\begin{array}{rcl} C(\textit{Berechnung von } u_1, \ldots, u_m) & = & O\left(m 2^{10n} n^4 Q^4\right) \\ & = & O\left(2^{11n} n^4 Q^4\right). \end{array}}$$

Wir implementieren den gesamten Algorithmus 3.4.6 in der Prozedur GANZHEITSBASIS. Der Output sind die Elemente $u_1, \ldots, u_m$, die eine Ganzheitsbasis für F_n/F_0 bilden, und ihre Bewertungen, bzw. Polordnungen ganzzahlig und modulo m an der Stelle $P_\infty^{(n)} \in \mathbb{P}_{F_n}$. Im Laufe dieser Prozedur werden die drei Hilfsprozeduren TMENGE, DIVSYS und DEFONE aufgerufen. Die Durchfürung des Maple 7 Befehls "Factor mod p" in dieser Prozedur ist nicht notwendig und kann bei den Berechnungen weggelassen werden. Die Faktorisierungen von $c_{(i,k)}$ für $i = 1, \ldots, k$ dienen nur einer besseren optischen Darstellung. Wir setzen zusätzlich $c_{(i,k)} := 0$ für $i = k+1, \ldots, m-1$, da es für den Ablauf der Hilfsprozedur DEFONE erforderlich ist. Die Prozedur DEFONE wird in den Prozeduren GANZHEITSBASIS und VPOLORDNUNGEN (wird im nächsten Abschnitt beschrieben) aufgerufen.

```
GANZHEITSBASIS := proc()
    local i, k, s, a, eqt, N, LGS1, LGS2;
    global A, c, e, u, val, mval;
    c(1, 1) := D||1;
    N||1 := degree(c(1, 1));
    for k from 2 to m-1 do
        e := array(1..k, 0..maxdeg);
        a||k := sum('e[k, s]* x||0^s', 's' = 0..degree(D||k));
        A||k := sum('e[k, s]*x||0^(Qs)', 's' = 0..degree(D||k));
        TMenge(w||k);
        for i from 1 to k - 1 do
            if ((Test = true) and (member(w||i, tmenge) = true)) or
            (Test = false) then
                a||i := sum('e[i, s]*x||0^s' , 's' = 0..N||i - 1);
                A||i := sum('e[i, s]*x||0^(Qs)', 's' = 0..N||i - 1);
            else
                a||i := 0;
                A||i := 0;
            end if;
        end do;
        LGS1 := DivSys(k);
        for i from 1 to k do
            if a|| i <> 0 then
                a||i := subs(LGS1, a||i) mod p;
            end if;
        end do;
        c(k, k) := Factor(Gcd(a||k, D||k) mod p) mod p;
        N||k := degree(c(k, k));
        eqt := {};
        for s from 0 to N||k do
            eqt := eqt union {coeff(a||k, x||0, s) = coeff(c(k, k), x||0, s)};
```

```
        end do;
        for s from N||k + 1 to degree(a||k) do
            eqt := eqt union {coeff(a||k, x||0, s) = 0};
        end do;
        LGS2 := msolve(eqt, p);
        for i from 1 to k - 1 do
            if a||i <> 0 then
                c(i, k) := Factor(subs(LGS2, a||i) mod p) mod p;
            else
                c(i, k) := 0;
            end if;
        end do;
    end do;
    for k from 1 to m-1 do
        for i from k + 1 to m - 1 do
            c(i, k) := 0;
        end do;
        DefOne(k);
    end do;
    u||m := 1;
    val||m := 0;
    mval||m := 0;
end proc;

DefOne := proc(k)
    local i, U, ValU;
    global u, val, mval;
    for i from 1 to m - 1 do
        U(i, k) := c(i, k)*'w'||i;
        ValU(i, k) := infval||i - m*degree(c(i, k));
    end do;
    u||k := sum('U(i, k)', 'i' = 1..m - 1);
    val||k := min(seq(ValU(i, k), i = 1..m - 1));
    mval||k := val||k mod m;
end proc;
```

4.4.9 Berechnung einer Ganzheitsbasis für F_n/F_0 mit modulo m paarweise inkongruenten Polordnungen an der Stelle $P_\infty^{(n)}$

Da die Implementierung von Algorithmus 3.5.3 mit seiner abstrakten Beschreibung in Abschnitt 3.5 übereinstimmt, geben wir gleich die entsprechende Prozedur VPOLORDNUNGEN an. Zur Komplexität ist noch folgendes zu sagen. Aus dem Beweis von Lemma 3.5.4 folgt, dass nach weniger als S_0 (siehe die dort eingeführten Bezeichnungen) Schritten der Algorithmus 3.5.3 endet. Daher schätzen wir S_0 ab:

$$\begin{aligned} S_0 &= \sum_{k=1}^{m} |v_{P_\infty^{(n)}}(u_k)| \\ &\leq \sum_{k=1}^{m} m \cdot max\{deg\ c_{(i,k)} \mid i = 1, \ldots, k\} \quad \text{wegen } u_k = \sum_{i=1}^{k} c_{(i,k)} w_i \end{aligned}$$

$$\begin{aligned}
&\leq \sum_{k=1}^{m} m \cdot max\{deg\ c_{(i,i)} \mid i = 1, \ldots, k\} && \text{nach Lemma 3.4.5}\\
&\leq \sum_{k=1}^{m} m \left(4\left(\frac{N_0^{(0)}}{Q} + 2^{n-1} + 2\right)\right) && \text{nach (52), (Seite 67)}\\
&\in O\left(m^2 4^n n\right) && \text{nach Lemma 4.4.5.5}\\
&= O\left(2^{4n} n\right).
\end{aligned}$$

Die Suche nach Indizes k_1 und k_2 erfordet Zeit, die nicht schlechter als $O(m^2)$ ist, die Suche nach dem Index s erfordet Zeit, die nicht schlechter als $O(m)$ ist. Die Berechnung (gegebenenfalls) eines neuen Ganzheitsbasiselements

if $deg\ c_{(s,k_1)} \leq deg\ c_{(s,k_2)}$
$\quad u_{k_2} = u_{k_2} - \frac{lcoefficient(c_{(s,k_2)})}{lcoefficient(c_{(s,k_1)})}\ x_0^{deg\ c_{(s,k_2)} - deg\ c_{(s,k_1)}} u_{k_1}$
else
$\quad u_{k_1} = u_{k_1} - \frac{lcoefficient(c_{(s,k_1)})}{lcoefficient(c_{(s,k_2)})}\ x_0^{deg\ c_{(s,k_1)} - deg\ c_{(s,k_2)}} u_{k_2}$
end if

benötigt höchtens (wegen des Substraktion der Polynome) Zeit

$$O(m \cdot max\{deg\ c_{(i,k)} \mid i = 1, \ldots, k\}) = O\left(m 4^n n\right) = O\left(2^{3n} n\right).$$

Damit gilt

$$\boxed{C(Algorithmus\ 3.5.3) = O\left(2^{7n} n^2\right).}\ ^{37}$$

In der Prozedur VPolordnungen wird (gegebenenfalls) eine weitere Ganzheitsbasis mit Elementen mit modulo m paarweise inkongruenten Polordnungen an der Stelle $P_\infty^{(n)}$ berechnet.

Es ist noch folgendes zu bemerken: nach Algorithmus 3.4.6 wird jedes u_k als $\sum_{i=1}^{k} c_{(i,k)} w_k$ konstruiert. Für $k < m$ gilt $w_i \notin \mathbb{F}_p$ für $i = 1, \ldots, k$. Damit folgt $v_{P_\infty^{(n)}}(u_k) \not\equiv 0\ mod\ m$ für $k = 1, \ldots, m-1$. Da $u_m = 1$, betrachten wir in dieser Prozedur nur $u_1, \ldots, u_{m-1}$. Die Durchführung des Maple 7 Befehls "Factor mod p" in dieser Prozedur ist nicht notwendig und kann bei den Berechnungen weggelassen werden. Die Faktorisierugen von Polynomen aus $\mathbb{F}_p[x_0]$ dienen nur einer besseren optischen Darstellung.

```
VPolordnungen := proc()
    local k1, k2, flag1, flag2, i, s;
    flag1 := false;
    while (flag1 = false) do
        k1 := 1;
        flag1 := true;
        while ((flag1 = true) and (k1 < m)) do
            k2 := k1 + 1;
            while ((flag1 = true) and (k2 < m)) do
                if mval||k1 = mval||k2 then
                    flag1 := false;
```

[37] Diese Komplexität entspricht dem Fall, wenn $S_i - S_{i-1} = 1$ für $i \geq 0$ gilt. Dies ist aber in den berechneten Beispielen nicht vorgekommen.

```
                else
                    k2 := k2 + 1;
                end if;
            end do;
            if flag1 = true then
                k1 := k1 + 1;
            end if;
        end do;
        if flag1 = false then
            flag2 := true;
            s := 1;
            while (flag2 = true) do
                if (mval||k1 = (infval||s mod m)) then
                    flag2 := false;
                else
                    s := s + 1;
                end if;
            end do;
            if degree(c(s, k1)) <= degree(c(s, k2)) then
                u||k2 := (u||k2 - (lcoeff(c(s, k2))/lcoeff(c(s, k1))) *
                x||0^(degree(c(s, k2)) - degree(c(s, k1)))* u||k1) mod p;
                for i from 1 to m - 1 do
                    c(i, k2) := Factor(coeff(u||k2, 'w'||i)) mod p;
                end do;
                DefOne(k2);
            else
                u||k1 := (u||k1 - (lcoeff(c(s, k1))/lcoeff(c(s, k2))) *
                x||0^(degree(c(s, k1)) - degree(c(s, k2)))* u||k2) mod p;
                for i from 1 to m - 1 do
                    c(i, k1) := Factor(coeff(u||k1, 'w'||i)) mod p;
                end do;
                DefOne(k1);
            end if;
        end if;
    end do;
end proc;
```

4.4.10 Berechnung einer Basis von $\mathcal{L}\left(rP_\infty^{(n)}\right)$

Nach Schritt 8 in Algorithmus 3.4.6 berechnen wir eine Basis von $\mathcal{L}\left(rP_\infty^{(n)}\right)$. Alle $v_{P_\infty^{(n)}}(u_i)$ sind bekannt, und wir können Proposition 3.6.1 anwenden.

$$
\begin{aligned}
&Basis\left(\mathcal{L}\left(rP_\infty^{(n)}\right)\right) = \{\}\\
&\text{for } i = 1,\ldots,m\\
&\quad \text{for } j = 0,\ldots,\left\lfloor \frac{r+v_{P_\infty^{(n)}}(u_i)}{m}\right\rfloor\\
&\qquad Basis\left(\mathcal{L}\left(rP_\infty^{(n)}\right)\right) = Basis\left(\mathcal{L}\left(rP_\infty^{(n)}\right)\right) \cup \left\{x_0^j u_i\right\}\\
&\quad \text{end for}\\
&\text{end for}
\end{aligned}
$$

Da $v_{P_\infty^{(n)}}(u_i) \leq 0$ für $i = 1, \ldots, m$ und r beliebig groß sein kann, folgt

$$\boxed{\begin{array}{rcl} C\left(\textit{Berechnung einer Basis von } \mathcal{L}\left(rP_\infty^{(n)}\right)\right) & = & O(max\{m, r\}) \\ & = & O\left(max\left\{2^n, r\right\}\right). \end{array}}$$

```
LBasis := proc()
    local i, j;
    global basis;
    basis := {};
    for i from 1 to m do
        for j from 0 to floor((r + val||i)/m) do
            basis := basis union {x||0^j * 'u'||i};
        end do;
    end do;
end proc;
```

4.4.11 Die Komplexität des Algorithmus 3.9.1 in Abhängigkeit von der Anzahl der rationalen Stellen von $F_n/\mathbb{F}_{p^2}$

Die Gesamtkomplexität des Algorithmus 3.9.1 zur Berechnung einer Basis von $\mathcal{L}\left(rP_\infty^{(n)}\right)$ wird in die Komplexität C_1 der Berechnung einer Ganzheitsbasis für die Funktionenkörpererweiterung F_n/F_0 mit modulo m paarweise inkongruenten Polordnungen an der Stelle $P_\infty^{(n)}$ und in die Komplexität C_2 der Anwendung von Proposition 3.6.1 zerlegt. Nach den Ergebnissen aus den Abschnitten 4.4.3 - 4.4.9, und da $Q = p^a < p \cdot 2^{2n}$ (siehe Abschnitt 4.4.4) gilt, folgt

$$C_1 = O\left(2^{11n} n^5 Q^4\right) = O\left(2^{19n} p^4 n^5\right).$$

Sei $N(F_n)$ die Anzahl der rationalen Stellen von $F_n/\mathbb{F}_{p^2}$. Nach [Gar-Sti-Rüc] sind genau $2(p-1)$ rationale Stellen von $F_0/\mathbb{F}_{p^2}$ voll zerlegt in $\mathcal{F}$. Daher folgt $N(F_n) \geq 2^{n+1}(p-1)$, und damit gilt

$$C_1 = O\left(N(F_n)^{19} \cdot log^5 N(F_n)\right).$$

Nach Abschnitt 4.4.10 gilt:

$$C_2 = O\left(max\left\{N(F_n), r\right\}\right).$$

Damit ist

$$C\left(\textit{Berechnung einer Basis von } \mathcal{L}\left(rP_\infty^{(n)}\right)\right) = O\left(N(F_n)^{19} \cdot log^5 N(F_n) + r\right).$$

4.4.12 Ein Beispiel

In diesem Abschnitt berechnen wir mittels des Programms eine Basis des Vektorraums $\mathcal{L}\left(P_\infty^{(n)}\right)$ für gewisse Inputparameter: n, p, r.

Den Output der Prozedur Basisdarstellung (die Basisdarstellungen von $w_1^Q, \ldots, w_m^Q$) geben wir ohne explizite Angabe der Koeffizienten $b_{ij} \in \mathbb{F}_p(x_0)$

für $i,j = 1,\ldots,m-1$ ($w_m = 1$). Wir können diese Koeffizienten aber jederzeit nach dem Ablauf der Prozedur Basisdarstellung durch Aufruf von $b(i,j)$ für $(i,j) \in \{1,\ldots,m-1\} \times \{1,\ldots,m-1\}$ ansehen. Den Output der Prozedur TMengen geben wir durch die Symbole $w_1,\ldots,w_m$ an.

Input: $p = 7$, $n = 4$, $r = 39$

Basis():

$$
\begin{aligned}
w_1 &= \frac{x_1x_2x_3x_4}{(x_0^2+1)(x_0+1)(x_0+6)^6} & v_{P_\infty^4}(w_1) &= 129\\
w_2 &= \frac{x_1x_3x_4}{(x_0^2+1)(x_0+6)^6} & v_{P_\infty^4}(w_2) &= 117\\
w_3 &= \frac{x_2x_3x_4}{(x_0+1)(x_0+6)^6} & v_{P_\infty^4}(w_3) &= 105\\
w_4 &= \frac{x_1x_2x_4}{(x_0^2+1)(x_0+1)(x_0+6)^4} & v_{P_\infty^4}(w_4) &= 99\\
w_5 &= \frac{x_3x_4}{(x_0+6)^6} & v_{P_\infty^4}(w_5) &= 93\\
w_6 &= \frac{x_1x_4}{(x_0^2+1)(x_0+6)^4} & v_{P_\infty^4}(w_6) &= 87\\
w_7 &= \frac{x_2x_4}{(x_0+1)(x_0+6)^4} & v_{P_\infty^4}(w_7) &= 75\\
w_8 &= \frac{x_1x_2x_3}{(x_0^2+1)(x_0+1)(x_0+6)^2} & v_{P_\infty^4}(w_8) &= 66\\
w_9 &= \frac{x_4}{(x_0+6)^4} & v_{P_\infty^4}(w_9) &= 63\\
w_{10} &= \frac{x_1x_3}{(x_0^2+1)(x_0+6)^2} & v_{P_\infty^4}(w_{10}) &= 54\\
w_{11} &= \frac{x_2x_3}{(x_0+1)(x_0+6)^2} & v_{P_\infty^4}(w_{11}) &= 42\\
w_{12} &= \frac{x_1x_2}{(x_0^2+1)(x_0+1)} & v_{P_\infty^4}(w_{12}) &= 36\\
w_{13} &= \frac{x_3}{(x_0+6)^2} & v_{P_\infty^4}(w_{13}) &= 30\\
w_{14} &= \frac{x_1}{x_0^2+1} & v_{P_\infty^4}(w_{14}) &= 24\\
w_{15} &= \frac{x_2}{x_0+1} & v_{P_\infty^4}(w_{15}) &= 12\\
w_{16} &= 1 & v_{P_\infty^4}(w_{16}) &= 0
\end{aligned}
$$

ZahlQ():

$$Q = 49$$

Basisdarstellung():

$$
\begin{aligned}
w_1^{27} &= b_{11}w_1 + b_{12}w_2 + b_{13}w_3 + b_{15}w_5\\
w_2^{27} &= b_{21}w_1 + b_{22}w_2 + b_{23}w_3 + b_{25}w_5\\
w_3^{27} &= b_{31}w_1 + b_{32}w_2 + b_{33}w_3 + b_{35}w_5\\
w_4^{27} &= b_{44}w_4 + b_{46}w_6 + b_{47}w_7 + b_{49}w_9
\end{aligned}
$$

$$
\begin{aligned}
w_5^{27} &= b_{51}w_1 + b_{52}w_2 + b_{53}w_3 + b_{55}w_5 \\
w_6^{27} &= b_{64}w_4 + b_{66}w_6 + b_{67}w_7 + b_{69}w_9 \\
w_7^{27} &= b_{74}w_4 + b_{76}w_6 + b_{77}w_7 + b_{79}w_9 \\
w_8^{27} &= b_{88}w_8 + b_{811}w_{11} \\
w_9^{27} &= b_{94}w_4 + b_{96}w_6 + b_{97}w_7 + b_{99}w_9 \\
w_{10}^{27} &= b_{1010}w_{10} + b_{1013}w_{13} \\
w_{11}^{27} &= b_{118}w_8 + b_{1111}w_{11} \\
w_{12}^{27} &= b_{1212}w_{12} \\
w_{13}^{27} &= b_{1310}w_{10} + b_{1313}w_{13} \\
w_{14}^{27} &= b_{1414}w_{14} \\
w_{15}^{27} &= b_{1515}w_{15} \\
w_{16}^{27} &= 1
\end{aligned}
$$

DPOLYNOME():

$$
\begin{aligned}
D_1 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^6 \\
D_2 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^6 \\
D_3 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^6 \\
D_4 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^5 \\
D_5 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^6 \\
D_6 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^5 \\
D_7 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^5 \\
D_8 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^2 \\
D_9 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^5 \\
D_{10} &= x_0(x_0+1)(x_0^2+1)(x_0+6)^2 \\
D_{11} &= x_0(x_0+1)(x_0^2+1)(x_0+6)^2 \\
D_{12} &= x_0(x_0^2+1) \\
D_{13} &= x_0(x_0+1)(x_0^2+1)(x_0+6)^2 \\
D_{14} &= x_0(x_0^2+1) \\
D_{15} &= x_0(x_0^2+1) \\
D_{16} &= 1
\end{aligned}
$$

TMENGEN():

$$
\begin{aligned}
T_1 &= \{w_1, w_2, w_3, w_5\} \\
T_2 &= \{w_4, w_6, w_7, w_9\} \\
T_3 &= \{w_8, w_{11}\} \\
T_4 &= \{w_{10}, w_{13}\} \\
T_5 &= \{w_{12}\} \\
T_6 &= \{w_{14}\} \\
T_7 &= \{w_{15}\} \\
T_8 &= \{w_{16}\}
\end{aligned}
$$

DisjunktTest():

"Die Indexmengen sind paarweise disjunkt"

Ganzheitsbasis():

$$\begin{aligned}
u_1 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^6 w_1\\
&\quad |v_{P_\infty^4}(u_1)| = 31\\
&\quad |v_{P_\infty^4}(u_1)| \equiv 15 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_2 &= 5x_0(x_0+1)(x_0^2+1)(x_0+6)^5 w_1 + x_0(x_0+1)(x_0^2+1)(x_0+6)^5 w_2\\
&\quad |v_{P_\infty^4}(u_2)| = 27\\
&\quad |v_{P_\infty^4}(u_2)| \equiv 11 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_3 &= 5x_0(x_0+1)(x_0^2+1)(x_0+6)^5 w_1 + x_0(x_0+1)(x_0^2+1)(x_0+6)^5 w_3\\
&\quad |v_{P_\infty^4}(u_3)| = 39\\
&\quad |v_{P_\infty^4}(u_3)| \equiv 7 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_4 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^5 w_4\\
&\quad |v_{P_\infty^4}(u_4)| = 45\\
&\quad |v_{P_\infty^4}(u_4)| \equiv 13 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_5 &= 3x_0(x_0+1)^4(x_0^2+1)(x_0+6)^2 w_1 + 4x_0(x_0+1)^3(x_0^2+1)(x_0+6)^2 w_2\\
&\quad + 6x_0(x_0+1)^2(x_0^2+1)(x_0+6)^2 w_3 + x_0(x_0+1)(x_0^2+1)(x_0+6)^2 w_5\\
&\quad |v_{P_\infty^4}(u_5)| = 15\\
&\quad |v_{P_\infty^4}(u_5)| \equiv 15 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_6 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^5 w_6\\
&\quad |v_{P_\infty^4}(u_6)| = 57\\
&\quad |v_{P_\infty^4}(u_6)| \equiv 9 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_7 &= 2x_0(x_0+1)(x_0^2+1)(x_0+6)^4 w_4 + x_0(x_0+1)(x_0^2+1)(x_0+6)^4 w_7\\
&\quad |v_{P_\infty^4}(u_7)| = 53\\
&\quad |v_{P_\infty^4}(u_7)| \equiv 5 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_8 &= x_0(x_0+1)(x_0^2+1)(x_0+6)^2 w_8\\
&\quad |v_{P_\infty^4}(u_8)| = 30\\
&\quad |v_{P_\infty^4}(u_8)| \equiv 14 \ mod\ 16
\end{aligned}$$

$$\begin{aligned}
u_9 &= x_0(x_0+1)(x_0^2+1)(x_0^4+6x_0^3+x_0^2+5x_0+4) w_4\\
&\quad + 3x_0^2(x_0+1)(x_0^2+1)(x_0+4)(x_0+3)^2 w_6 + 6x_0(x_0+1)^2(x_0^2+1) w_7\\
&\quad + x_0(x_0+1)(x_0^2+1) w_9
\end{aligned}$$

$$|v_{P^4_\infty}(u_9)| = 41$$
$$|v_{P^4_\infty}(u_9)| \equiv 9 \ mod \ 16$$

$$\begin{aligned} u_{10} &= x_0(x_0+1)(x_0^2+1)(x_0+6)^2 w_{10} \\ & |v_{P^4_\infty}(u_{10})| = 42 \\ & |v_{P^4_\infty}(u_{10})| \equiv 10 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{11} &= 5x_0^2(x_0+1)(x_0^2+1)w_8 + x_0(x_0+1)(x_0^2+1)w_{11} \\ & |v_{P^4_\infty}(u_{11})| = 22 \\ & |v_{P^4_\infty}(u_{11})| \equiv 6 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{12} &= x_0(x_0^2+1)w_{12} \\ & |v_{P^4_\infty}(u_{12})| = 12 \\ & |v_{P^4_\infty}(u_{12})| \equiv 12 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{13} &= 5x_0^2(x_0+1)(x_0^2+1)w_{10} + x_0(x_0+1)(x_0^2+1)w_{13} \\ & |v_{P^4_\infty}(u_{13})| = 34 \\ & |v_{P^4_\infty}(u_{13})| \equiv 2 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{14} &= x_0(x_0^2+1)w_{14} \\ & |v_{P^4_\infty}(u_{14})| = 24 \\ & |v_{P^4_\infty}(u_{14})| \equiv 8 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{15} &= x_0(x_0^2+1)w_{15} \\ & |v_{P^4_\infty}(u_{15})| = 36 \\ & |v_{P^4_\infty}(u_{15})| \equiv 4 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{16} &= w_{16} \\ & |v_{P^4_\infty}(u_{16})| = 0 \\ & |v_{P^4_\infty}(u_{16})| \equiv 0 \ mod \ 16 \end{aligned}$$

VPOLORDNUNGEN():

$$\begin{aligned} u_1 &= 3x_0(x_0+1)(x_0+6)^2(x_0^2+1)(x_0^2+3x_0+5)w_1 \\ &+ x_0^2(x_0+1)^3(x_0+6)^2(x_0^2+1)w_2 + 5x_0^2(x_0+1)^2(x_0^2+1)(x_0+6)^2 w_3 \\ &+ 2x_0^2(x_0+6)^2(x_0^2+1)(x_0+1)w_5 \\ & |v_{P^4_\infty}(u_1)| = 27 \\ & |v_{P^4_\infty}(u_1)| \equiv 11 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_2 &= 5x_0(x_0+1)^2(x_0^2+1)(x_0+6)^2(x_0^2+x_0+3)w_1 \\ &+ 2x_0(x_0+6)^2(x_0^2+1)(x_0+1)(x_0^2+x_0+3)w_2 \end{aligned}$$

$$
\begin{aligned}
& + 2x_0^2(x_0+1)^2(x_0^2+1)(x_0+6)^2w_3 + 5x_0^2(x_0+6)^2(x_0^2+1)(x_0+1)w_5\\
& |v_{P_\infty^4}(u_2)| = 23\\
& |v_{P_\infty^4}(u_2)| \equiv 7 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_3 \;=\;& x_0(x_0+1)(x_0+3)(x_0^3+4x_0^2+5x_0+3)(x_0+6)^2(x_0^2+1)w_1\\
& + 6x_0^2(x_0+6)^2(x_0^2+1)(x_0+1)(x_0^2+x_0+3)w_2\\
& + 3x_0(x_0+6)^2(x_0^2+1)(x_0+1)(x_0+4)^2w_3\\
& + x_0^3(x_0+6)^2(x_0^2+1)(x_0+1)w_5\\
& |v_{P_\infty^4}(u_3)| = 35\\
& |v_{P_\infty^4}(u_3)| \equiv 3 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_4 \;=\;& 3x_0(x_0+1)(x_0+6)(x_0^2+1)(x_0^2+3x_0+5)w_4\\
& + x_0^2(x_0+1)^3(x_0+6)(x_0^2+1)w_6 + 5x_0^2(x_0+1)^2(x_0+6)(x_0^2+1)w_7\\
& + 2x_0^2(x_0+1)(x_0+6)(x_0^2+1)w_9\\
& |v_{P_\infty^4}(u_4)| = 41\\
& |v_{P_\infty^4}(u_4)| \equiv 9 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_5 \;=\;& 3x_0(x_0+1)^4(x_0+6)^2(x_0^2+1)w_1 + 4x_0(x_0+1)^3(x_0+6)^2(x_0^2+1)w_2\\
& + 6x_0(x_0^2+1)(x_0+6)^2(x_0+1)^2w_3 + x_0(x_0+1)(x_0^2+1)(x_0+6)^2w_5\\
& |v_{P_\infty^4}(u_5)| = 15\\
& |v_{P_\infty^4}(u_5)| \equiv 15 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_6 \;=\;& x_0(x_0+1)^2(x_0+2)(x_0+5)^2(x_0^2+1)w_4\\
& + 6x_0(x_0+1)(x_0+2)(x_0+5)^2(x_0^2+1)w_6 + 5x_0^3(x_0+1)^2(x_0^2+1)w_7\\
& + 2x_0^3(x_0+1)(x_0^2+1)w_9\\
& |v_{P_\infty^4}(u_6)| = 37\\
& |v_{P_\infty^4}(u_6)| \equiv 5 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_7 \;=\;& 4x_0(x_0+1)(x_0^2+1)(x_0^5+3x_0^4+6x_0^3+6x_0+4)w_4\\
& + 3x_0^2(x_0+1)(x_0^2+1)(x_0+2)(x_0+5)^2w_6\\
& + 2x_0(x_0+1)(x_0^2+1)(x_0^3+3x_0^2+5x_0+4)w_7 + x_0^4(x_0^2+1)(x_0+1)w_9\\
& |v_{P_\infty^4}(u_7)| = 49\\
& |v_{P_\infty^4}(u_7)| \equiv 1 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_8 \;=\;& x_0(x_0^2+1)(x_0+6)^2(x_0+1)w_8\\
& |v_{P_\infty^4}(u_8)| = 30\\
& |v_{P_\infty^4}(u_8)| \equiv 14 \ mod\ 16
\end{aligned}
$$

$$
\begin{aligned}
u_9 \;=\;& 4x_0(x_0+1)^4(x_0^2+1)(x_0+6)w_4 + 3x_0(x_0+1)^3(x_0^2+1)(x_0+6)w_6\\
& + x_0(x_0+1)^2(x_0^2+1)(x_0+6)w_7 + 6x_0(x_0+1)(x_0^2+1)(x_0+6)w_9
\end{aligned}
$$

$$|v_{P^4_\infty}(u_9)| = 29$$
$$|v_{P^4_\infty}(u_9)| \equiv 13 \ mod \ 16$$

$$\begin{aligned} u_{10} &= x_0(x_0^2+1)(x_0+6)^2(x_0+1)w_{10} \\ &|v_{P^4_\infty}(u_{10})| = 42 \\ &|v_{P^4_\infty}(u_{10})| \equiv 10 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{11} &= 5x_0^2(x_0^2+1)(x_0+1)w_8 + x_0(x_0^2+1)(x_0+1)w_{11} \\ &|v_{P^4_\infty}(u_{11})| = 22 \\ &|v_{P^4_\infty}(u_{11})| \equiv 6 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{12} &= x_0(x_0^2+1)w_{12} \\ &|v_{P^4_\infty}(u_{12})| = 12 \\ &|v_{P^4_\infty}(u_{12})| \equiv 12 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{13} &= 5x_0^2(x_0^2+1)(x_0+1)w_{10} + x_0(x_0^2+1)(x_0+1)w_{13} \\ &|v_{P^4_\infty}(u_{13})| = 34 \\ &|v_{P^4_\infty}(u_{13})| \equiv 2 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{14} &= x_0(x_0^2+1)w_{14} \\ &|v_{P^4_\infty}(u_{14})| = 24 \\ &|v_{P^4_\infty}(u_{14})| \equiv 8 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{15} &= x_0(x_0^2+1)w_{15} \\ &|v_{P^4_\infty}(u_{15})| = 36 \\ &|v_{P^4_\infty}(u_{15})| \equiv 4 \ mod \ 16 \end{aligned}$$

$$\begin{aligned} u_{16} &= w_{16} \\ &|v_{P^4_\infty}(u_{16})| = 0 \\ &|v_{P^4_\infty}(u_{16})| \equiv 0 \ mod \ 16 \end{aligned}$$

LBASIS():

$$\left\{ \begin{array}{c} u_1, u_2, x_0u_2, u_3, u_5, x_0u_5, u_6, u_8, u_9, u_{11}, x_0u_{11}, \\ u_{12}, x_0u_{12}, u_{13}, u_{14}, u_{15}, u_{16}, x_0u_{16}, x_0^2u_{16} \end{array} \right\}$$

5 Kummersche Erweiterungen $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ mit vielen rationalen Stellen für $Char\ \mathbb{F}_q = 2$

Theorem 5.1 *Sei $q = 2^m$, $m \geq 2$. Sei $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ eine Kummersche Funktionenkörpererweiterung vom Grad $q-1$ mit der definierenden Gleichung*

$$y^{q-1} = f(x) \in \mathbb{F}_q(x).$$

Dann sind das Geschlecht g' und die Anzahl der rationalen Stellen N von $\mathbb{F}_q(x,y)/\mathbb{F}_q$ aus der folgenden Tabelle abzulesen:

Fall	*Voraussetzungen*	g'	N	$N/g' >$
1.	$m \equiv 0\ mod\ 2,\ m \geq 6,$ $f(x) = \frac{x^{q-1}+1}{x^3+1} + 1$	$\frac{1}{8}(q^2 - 6q - 32)$	$(q-1)(q-4)+15$	8
2.	$m \equiv 0\ mod\ 2,\ m \geq 4,$ $f(x) = x^d(x^d+1),$ *wobei* $d = \frac{q-1}{3}$ *ist*	$\frac{1}{6}(q^2 - 5q + 10)$	$\frac{1}{3}(2q+1)(q-1)$	4
3.	$m \equiv 1\ mod\ 2,$ $f(x) = \frac{(x^{2^{m-s}}+x+1)^{2^s}}{x^{2^s}+x+1},$ *wobei* $s = \frac{m-1}{2}$ *ist*	$\frac{1}{2}(q-2)(3\cdot 2^s - 1)$	$q(q-1)+1$	$\frac{2\sqrt{2}}{3}\sqrt{q}$
4.	$m \equiv 0\ mod\ 4,$ $f(x) = \frac{(x^{2^{m-s}}+x+1)^{2^s}}{x^{2^s}+x+1},$ *wobei* $s = \frac{m}{2} - 1$ *ist*	$\frac{1}{2}(q-2)(5\cdot 2^s - 3)$	$(q-2)(q-1)+3$	$\frac{4}{5}\sqrt{q}$
5.	$m \equiv 2\ mod\ 4,\ m \geq 6$ $f(x) = \frac{(x^{2^{m-s}}+x+1)^{2^s}}{x^{2^s}+x+1},$ *wobei* $s = \frac{m}{2} - 1$ *ist*	$\frac{1}{2}(q-2)(5\cdot 2^s - 1) - 1$	$q(q-1)+3$	$\frac{4}{5}\sqrt{q}$

Beweis. Für den Beweis unterscheiden wir wie in der Tabelle fünf Fälle. Im weiteren bei genauer Betrachtung jedes Falls werden wir feststellen, dass eine Stelle von $\mathbb{F}_q(x)/\mathbb{F}_q$ existiert, die voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ ist. Daher werden wir Folgerung 2.2.18 anwenden, für die unter den Voraussetzungen des Theorems gilt

$$F = \mathbb{F}_q(x),\ F' = \mathbb{F}_q(x,y),\ g = 0,\ n = q-1,\ u = f(x),\ K = K' = \mathbb{F}_q,$$

und die Formel zur Berechnung von g' vereinfacht sich wie folgt

$$g' = 2 - q + \frac{1}{2} \sum_{P \in \mathbb{P}_{\mathbb{F}_q(x)}} (q - 1 - r_P) deg\ P,$$

wobei $r_P = ggT(q-1, v_P(f(x))) = \frac{q-1}{e(P'|P)}$ mit $P'|P$ ist. Sei

$$R := \sum_{P \in \mathbb{P}_{\mathbb{F}_q(x)}} (q - 1 - r_P) deg\ P.$$

Sei $l \in \mathbb{N}$. Sei E ein Körper und $\bar{E}$ sein algebraischer Abschluß. Sei $\mathcal{S}_l \subseteq \bar{E}$ die Menge primitiver l-ter Einheitswurzeln über E. Dann wird l-tes Kreisteilungspolynom mit $\phi_l(x) = \prod_{\xi \in \mathcal{S}_l}(x - \xi) \in \bar{E}[x]$ bezeichnet, und es gilt:

$$x^l - 1 = \prod_{d \mid l} \phi_d(x).$$

Sei $P_\infty \in \mathbb{P}_{\mathbb{F}_q(x)}$ der Pol des Elements x und $P_{p(x)} \in \mathbb{P}_{\mathbb{F}_q(x)}$ die Stelle, die durch das normierte irreduzible Polynom $p(x) \in \mathbb{F}_q[x]$ definiert ist. Dann sind die in der Tabelle angegebenen Fälle im weiteren wie folgt beschrieben.

FALL 1.

BEHAUPTUNG 1. Es gilt

$$\frac{x^{q-1}+1}{x^3+1} + 1 = x^3 \phi_1^3(x) \phi_3^3(x) \prod_{d \mid 2^{m-2}-1,\ d>3} \phi_d^4(x).$$

BEWEIS.

$$\begin{aligned} \frac{x^{q-1}+1}{x^3+1} + 1 &= \frac{x^{q-1}+x^3}{\phi_1(x)\phi_3(x)} = \frac{x^3\left((x^4)^{2^{m-2}-1}+1\right)}{\phi_1(x)\phi_3(x)} \\ &= \frac{x^3(x^{2^{m-2}-1}+1)^4}{\phi_1(x)\phi_3(x)} = \frac{x^3 \prod_{d \mid 2^{m-2}-1} \phi_d^4(x)}{\phi_1(x)\phi_3(x)}. \end{aligned}$$ ◁

Nach Behauptung 1 sieht die definierende Gleichung wie folgt aus:

$$y^{q-1} = x^3 \phi_1^3(x) \phi_3^3(x) \prod_{d \mid 2^{m-2}-1,\ d>3} \phi_d^4(x). \tag{53}$$

Wegen $m \equiv 0\ mod\ 2$ und $m \geq 6$ gilt $\mathbb{F}_q \cap \mathbb{F}_{2^{m-2}} = \mathbb{F}_{2^{ggT(m,m-2)}} = \mathbb{F}_4$. Daher hat das Polynom $\prod_{d \mid 2^{m-2}-1,\ d>3} \phi_d(x)$ keine Nullstellen in $\mathbb{F}_q$. Die durch es definierten Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ sind daher nicht rational, und sie sind voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ wegen $ggT(q-1,4) = 1$. So spielen diese Stellen nur bei der Berechnung des Geschlechts g' eine Rolle. Die Summe deren Grade ist:

$$deg \prod_{d \mid 2^{m-2}-1,\ d>3} \phi_d(x) = deg\left(\frac{x^{2^{m-2}-1}+1}{x^3+1}\right) = 2^{m-2} - 2^2 = \frac{1}{4}(q-16).$$

Damit ist einer der Summanden in R gleich $\frac{1}{4}(q-2)(q-16)$.

Wir schreiben die Gleichung (53) so um, dass wir über die Grade und über das Verzweigungsverhalten der anderen (durch diese Gleichung definierten) Stellen Aussagen machen können. Sei ξ eine primitive 3-te Einheitswurzel über $\mathbb{F}_2$, d.h. $\mathbb{F}_2(\xi) = \mathbb{F}_4 \subset \mathbb{F}_q$. Dann gilt:

$$y^{q-1} = x^3(x+1)^3(x+\xi)^3(x+(\xi+1))^3(x^{3(l-1)} + x^{3(l-2)} + \cdots + x^3 + 1)^4, \quad (54)$$

wobei $l := \frac{2^{m-2}-1}{3}$. Daher haben die Stellen P_x, P_{x+1}, $P_{x+\xi}$, $P_{x+(\xi+1)}$, P_∞ von $\mathbb{F}_q(x)/\mathbb{F}_q$ jeweils drei Fortsetzungen in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ und den Verzweigungsindex $\frac{q-1}{3}$. Wir zeigen dies am Beispiel von $P_{x+\xi}$.

Sei $z := \frac{y^{\frac{q-1}{3}}}{x+\xi}$. Dann folgt $\mathbb{F}_q(x) \subseteq \mathbb{F}_q(z) \subseteq \mathbb{F}_q(x,y)$, und wir betrachten die Erweiterung $\mathbb{F}_q(z)/\mathbb{F}_q(x)$ mit der definierenden Gleichung

$$z^3 = x^3(x+1)^3(x+(\xi+1))^3(\underbrace{x^{3(l-1)} + x^{3(l-2)} + \cdots + x^3 + 1}_{\text{ungerade Anzahl der Summanden}})^4.$$

Ist $x = \xi$, so gilt $z^3 = 1$. Da $z^3 - 1$ in drei paarweise verschiedene Faktoren über $\mathbb{F}_q \supset \mathbb{F}_4$ zerfällt, hat die Stelle $P_{x+\xi}$ drei Fortsetzungen in $\mathbb{F}_q(z)/\mathbb{F}_q(x)$.

Sei $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_4$. Dann gilt für $x = \alpha$

$$y^{q-1} = \frac{\alpha^{q-1}+1}{\alpha^3+1} + 1 = 1.$$

Daraus folgt, dass die $q-4$ rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ voll zerlegt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ sind.

Damit werden das Geschlecht g' und die Anzahl der rationalen Stellen N von $\mathbb{F}_q(x,y)/\mathbb{F}_q$ wie folgt berechnet:

$$g' = 2 - q + \frac{1}{2}\left(\frac{1}{4}(q-2)(q-16) + 5(q-4)\right) = \frac{1}{8}(q^2 - 6q - 32),$$

$$N = (q-4)(q-1) + 15.$$

Damit folgt ($q \geq 64$):

$$N/g' = 8\left(1 + \frac{8q+51}{q^2-6q-32}\right) > 8.$$

FALL 2.

BEHAUPTUNG 2. Sei $d = \frac{q-1}{3}$. Dann gilt

$$x^{2d} + x^d + 1 = \prod_{l \mid q-1,\ l \nmid d} \phi_l(x).$$

BEWEIS. Wegen $d = \frac{q-1}{3}$ gilt

$$\frac{x^{q-1}+1}{x^d+1} = x^{q-1-d} + x^{q-1-2d} + x^{q-1-3d} = x^{2d} + x^d + 1,$$

und da

$$x^{q-1}+1 = \prod_{l \mid q-1} \phi_l(x) = \prod_{l \mid d} \phi_l(x) \prod_{l \mid q-1,\ l \nmid d} \phi_l(x) = (x^d+1) \prod_{l \mid q-1,\ l \nmid d} \phi_l(x),$$

folgt die Behauptung. $\lhd$

Da $d \mid q-1$, zerfällt x^d+1 (aus der definierenden Gleichung für $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$) über $\mathbb{F}_q$ in d paarweise verschiedene lineare Faktoren. Damit sind die durch sie definierten d rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$.

Analog zu Überlegungen in Fall 1 folgt, dass die Stellen P_x und P_∞ jeweils den Verzweigungsindex 3 und d Fortsetzungen in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ haben.

Nach Behauptung 2 hat $x^{2d}+x^d+1$ paarweise verschiedene einfache Nullstellen $\beta_1,\ldots,\beta_{2d} \in \mathbb{F}_q^*$. Da $y^{q-1}=1$ für $x=\beta_i$ für $i=1,\ldots,2d$ gilt, folgt, dass diese $2d$ rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ voll zerlegt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ sind.

Unter Berücksichtigung von $d=\frac{q-1}{3}$ werden das Geschlecht g' und die Anzahl der rationalen Stellen N von $\mathbb{F}_q(x,y)/\mathbb{F}_q$ wie folgt berechnet:

$$g' = 2-q+\frac{1}{2}((q-2)d+(q-1-d)2) = \frac{1}{6}(q^2-5q+10),$$

$$N = 2d(q-1)+2d+d = \frac{1}{3}(2q+1)(q-1).$$

Damit folgt ($q \geq 16$):

$$N/g' = 4\left(1+\frac{4\frac{1}{2}q-10\frac{1}{2}}{q^2-5q+10}\right) > 4.$$

Für die nächsten drei Fälle brauchen wir ein Lemma.

Lemma 5.2 *Sei $f(x)=x^{2^n}+x+1 \in \mathbb{F}_q[x]$, $n \in \mathbb{N}$. Sei Char $\mathbb{F}_q = 2$. Dann gilt:*
(1) $f(x)$ hat alle Nullstellen in $\mathbb{F}_{2^{2n}} \setminus \mathbb{F}_2$ und ist quadratfrei.
(2) $x^2+x+1 \mid f(x)$, falls $n \equiv 1$ mod 2.

Beweis. (1) Wegen $x^{2^{2n}}+x = (x^{2^n}+x+1)^{2^n}+(x^{2^n}+x+1)$ gilt $f(x) \mid x^{2^{2n}}+x$. Da die erste Ableitung von $f(x)$ gleich 1 ist, hat $f(x)$ nur einfache Nullstellen in seinem Zerfällungskörper.
(2) $f(x)$ kann für $n \equiv 1$ *mod* 2 wie folgt dargestellt werden:

$$f(x) = x^{2^n}+x+1 = \sum_{k=1}^{n}(x^2+x+1)^{2^{n-k}}.$$

□

FALL 3.
Behauptung 3. Es gilt

$$\mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_{2^{2s}} = \mathbb{F}_4, \quad \mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_q = \mathbb{F}_2, \quad \mathbb{F}_{2^{2s}} \cap \mathbb{F}_q = \mathbb{F}_2.$$

Beweis. Wegen $s=\frac{m-1}{2}$ gilt $m-s=\frac{m+1}{2}$. Dann folgt $ggT(m-s,s)=1$, und damit gilt $\mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_{2^{2s}} = \mathbb{F}_{2^{2ggT(m-s,s)}} = \mathbb{F}_{2^2}$. Die anderen Aussagen folgen aus $ggT(m,2(m-s)) = ggT(m,m+1) = 1 = ggT(m,m-1) = ggT(m,2s)$. $\lhd$

Nach Behauptung 3 und Lemma 5.2 sind die Polynome $x^{2^{m-s}}+x+1$ und $x^{2^s}+x+1$ aus der definierenden Gleichung

$$y^{q-1} = \frac{(x^{2^{m-s}}+x+1)^{2^s}}{x^{2^s}+x+1}$$

teilerfremd, quadratfrei und haben keine Nullstellen in $\mathbb{F}_q$. Daher definieren sie[38] nur Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$, die nicht rational und nach der definierenden Gleichung voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ sind.

Da $ggT(2^m-2^s, q-1) = ggT(2^{m-s}-1, 2^m-1) = 1$, ist die Stelle P_∞ auch voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$.

Sei $\alpha \in \mathbb{F}_q^*$. Dann gilt für $x = \alpha$ wegen $q = 2^m$:

$$y^{q-1} = \frac{\alpha^{2^m} + \alpha^{2^s} + 1}{\alpha^{2^s} + \alpha + 1} = \frac{\alpha + \alpha^{2^s} + 1}{\alpha^{2^s} + \alpha + 1} = 1.$$

Für $x = 0$ gilt auch $y^{q-1} = 1$. Daraus folgt, dass die q rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ voll zerlegt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ sind.

Da $m - s = s + 1$ und $2^s = \sqrt{\frac{q}{2}}$ gilt, folgt

$$g' = 2 - q + \frac{1}{2}(2^{m-s} + 2^s + 1)(q-2) = \frac{1}{2}(q-2)(3 \cdot 2^s - 1),$$

$$N = q(q-1) + 1,$$

und damit ($q \geq 8$)

$$N/g' > \frac{2\sqrt{2}}{3}\sqrt{q}.$$

FALL 4.

BEHAUPTUNG 4. Es gilt

$$\mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_{2^{2s}} = \mathbb{F}_4, \quad \mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_q = \mathbb{F}_4, \quad \mathbb{F}_{2^{2s}} \cap \mathbb{F}_q = \mathbb{F}_4.$$

BEWEIS. Wegen $s = \frac{m}{2} - 1$ gilt $m - s = \frac{m}{2} + 1$. Damit, und da $m \equiv 0 \ mod\ 4$, folgt $ggT(m-s, s) = 1$, und damit gilt $\mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_{2^{2s}} = \mathbb{F}_{2^{2ggT(m-s,s)}} = \mathbb{F}_4$. Wegen $ggT(m, 2(m-s)) = ggT(m, m+2) = 2 = ggT(m, m-2) = ggT(m, 2s)$ gelten die anderen Aussagen. $\lhd$

Nach Behauptung 4 und Lemma 5.2 sind die Polynome $x^{2^{m-s}} + x + 1$ und $x^{2^s} + x + 1$ aus der definierenden Gleichung

$$y^{q-1} = \frac{(x^{2^{m-s}} + x + 1)^{2^s}}{x^{2^s} + x + 1}$$

quadratfrei, haben nur zwei gemeinsame Nullstellen, die in $\mathbb{F}_4 \setminus \mathbb{F}_2 \subset \mathbb{F}_q$ liegen, und keine weiteren Nullstellen in $\mathbb{F}_q$. Daher können die beiden Polynome durch $x^2 + x + 1$ geteilt werden, und die definierende Gleichung sieht danach wie folgt aus:

$$y^{q-1} = (x^2 + x + 1)^{2^s - 1} \frac{(x^{2^{m-s}-2} + \ldots + 1)^{2^s}}{x^{2^s-2} + \ldots + 1}.$$

Die Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$, die durch die Polynome[39] im Zähler und im Nenner des Quotienten in der letzten Darstellung definiert sind, sind nicht rational und voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$.

[38] Bzw. ihre über $\mathbb{F}_q$ paarweise verschiedenen nicht linearen Faktoren, falls diese Polynome in welche zerfallen.

[39] Bzw. durch ihre über $\mathbb{F}_q$ paarweise verschiedenen nicht linearen Faktoren, falls diese Polynome in welche zerfallen.

Die zwei rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$, die durch die Faktoren von x^2+x+1 definiert sind, und die Stelle P_∞ sind voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ wegen $ggT(2^m-2^s,q-1)=1$ (für P_∞) und $ggT(2^s-1,q-1)=1$.

Sei $\alpha \in \mathbb{F}_q \setminus \{\mathbb{F}_4 \setminus \mathbb{F}_2\}$. Dann gilt für $x=\alpha$ analog zu Fall 3: $y^{q-1}=1$. Daraus folgt, dass die $q-2$ rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ voll zerlegt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ sind.

Wegen $m-s=s+2$ und $2^s=\frac{\sqrt{q}}{2}$ gilt:

$$g' = 2-q+\frac{1}{2}(2^{m-s}-2+2^s-2+3)(q-2) = \frac{1}{2}(q-2)(5\cdot 2^s-3),$$

$$N=(q-2)(q-1)+3,$$

und damit ($q \geq 16$)

$$N/g' > \frac{4}{5}\sqrt{q}.$$

FALL 5.

Behauptung 5. Es gilt

$$\mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_{2^{2s}} = \mathbb{F}_{16}, \quad \mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_q = \mathbb{F}_4, \quad \mathbb{F}_{2^{2s}} \cap \mathbb{F}_q = \mathbb{F}_4.$$

Beweis. Wegen $s=\frac{m}{2}-1$ gilt $m-s=\frac{m}{2}+1$. Damit, und da $m \equiv 2 \ mod\ 4$ ist, folgt $ggT(m-s,s)=2$, und damit gilt $\mathbb{F}_{2^{2(m-s)}} \cap \mathbb{F}_{2^{2s}} = \mathbb{F}_{2^{2ggT(m-s,s)}} = \mathbb{F}_{2^4}$. Wegen $ggT(m,2(m-s)) = ggT(m,m+2) = 2 = ggT(m,m-2) = ggT(m,2s)$ gelten die anderen Aussagen. $\lhd$

Nach Behauptung 5 und Lemma 5.2 sind die Polynome $x^{2^{m-s}}+x+1$ und $x^{2^s}+x+1$ aus der definierenden Gleichung

$$y^{q-1} = \frac{(x^{2^{m-s}}+x+1)^{2^s}}{x^{2^s}+x+1}$$

quadratfrei, haben eventuell in $\mathbb{F}_{16}\setminus\mathbb{F}_4$ die gemeinsamen Nullstellen, aber keine Nullstellen in $\mathbb{F}_q$. Wir zeigen, dass diese beiden Polynome unter den Voraussetzungen dieses Falls keine gemeinsamen Nullstellen haben.

Existiert ein $\gamma \in \mathbb{F}_{16}\setminus\mathbb{F}_4$, so dass

$$x+\gamma \mid x^{2^{m-s}}+x+1 \text{ und } x+\gamma \mid x^{2^s}+x+1$$

gilt, so teilt $x+\gamma$ dann auch ihre Summe $x^{2^{m-s}}+x^{2^s}$. Damit folgt

$$x+\gamma \mid x^{2^{m-s}-2^s}+1,$$

und wegen $\gamma \in \mathbb{F}_{16}\setminus\mathbb{F}_4$ gilt

$$x+\gamma \mid x^{15}+1.$$

Nun berechnen wir

$$ggT(x^{15}+1, x^{2^{m-s}-2^s}+1) = (x^{ggT(15,3\cdot 2^s)}+1) = x^3+1 \in \mathbb{F}_4[x],$$

was ein Widerspruch zu $x+\gamma \notin \mathbb{F}_4[x]$ ist.

Alle durch diese Polynome[40] definierten Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ sind nicht rational und voll verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$.

Da $ggT(2^m-1, 2^m-2^s) = 2^{ggT(m,m-s)}-1 = 3$ gilt, ist die Stelle P_∞ verzweigt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ mit dem Verzweigungsindex $\frac{q-1}{3}$, und die Anzahl ihrer Fortsetzungen ist gleich 3.

Sei $\alpha \in \mathbb{F}_q$. Dann gilt für $x = \alpha$ analog zu Fall 3: $y^{q-1} = 1$. Daraus folgt, dass die q rationalen Stellen von $\mathbb{F}_q(x)/\mathbb{F}_q$ voll zerlegt in $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ sind.

Wegen $m - s = s + 2$ und $2^s = \frac{\sqrt{q}}{2}$ gilt:

$$g' = 2 - q + \frac{1}{2}((2^{m-s} + 2^s)(q-2) + (q-4)) = \frac{1}{2}(q-2)(5 \cdot 2^s - 1) - 1,$$

$$N = q(q-1) + 3,$$

und damit ($q \geq 64$)

$$N/g' > \frac{4}{5}\sqrt{q}.$$

□

In der folgenden Tabelle ist zu jedem Fall jeweils ein Beispiel angegeben. Die fett gedruckten Zahlen bedeuten eine neue Anzahl der rationalen Stellen im Vergleich zu [Gee-Vlu 1], eine in einer Box gedruckte Zahl ist gleich der Anzahl der rationalen Stellen in einem Beispiel in [Gee-Vlu 2], die zwei anderen Ergebnisse sind für die größeren Geschlechter (keine Vergleichsmöglichkeit).

Fall	q	Die definierende Gleichung	g'	N	N/g'
1.	64	$y^{63} = x^3(x+1)^3(x^2+x+1)^3\phi_5^4(x)\phi_{15}^4(x)$	460	3795	8,3
2.	16	$y^{15} = x^5(x^5+1) = x^5\phi_1(x)\phi_5(x)$	31	**165**	5,3
3.	8	$y^7 = (x^4+x+1)^2/(x^2+x+1)$	15	**57**	3,8
4.	16	$y^{15} = (x^2+x+1)(x^6+x^5+x^3+x^2+1)^2$	49	$\boxed{213}$	4,3
5.	64	$y^{63} = (x^{16}+x+1)^4/(x^4+x+1)$	588	4035	6,9

[40] Bzw. durch ihre über $\mathbb{F}_q$ paarweise verschiedenen nicht linearen Faktoren, falls diese Polynome in welche zerfallen.

Literatur

[Aho-Hop-Ull] A. Aho, J. Hopcroft, J. Ullman, *The Design and Analysis of Computer Algorithms*, Reading, Mass.: Addison-Wesley 1974.

[Ale] I. Aleshnikov, *Ganzheitsbasen in einem Turm algebraischer Funktionenkörper: ein Beitrag zur Konstruktion asymptotisch guter algebraisch-geometrischer Codes*, Dissertation, Universität Essen, 2000.

[Ale-Deo-Kum-Sti] I. Aleshnikov, V. Deolalikar, P. V. Kumar, H. Stichtenoth, *Towards a Basis for a Space of Regular Functions in a Tower of Function Fields Meeting the Drinfeld-Vlădut Bound*, 5th Int. Conf. Finite Fields and Applications, University of Augsburg, Germany, 1999.

[Elk] N. D. Elkies, *Explicit Modular Towers*, in Proc. 35tn. Annu. Allerton Conf. Communication, Control and Computing, Urbana, IL, 1997.

[Gar-Sti 1] A. Garcia, H. Stichtenoth, *A Tower of Artin-Schreier Extensions of Function Fields Attaining the Drinfeld-Vlădut Bound*, Invent. Math. 121, 1995, 211-222.

[Gar-Sti 2] A. Garcia, H. Stichtenoth, *On the Asymptotic Behavior of Some Towers of Function Fields over Finite Fields*, J. Number Theory 61, 1996, 248-273.

[Gar-Sti-Rüc] A. Garcia, H. Stichtenoth, H. Rück *On Tame Towers over Finite Fields*, Reine und Angewandte Mathematik 557, 2003, 53-80.

[Gar-Sti-Tho] A. Garcia, H. Stichtenoth, M. Thomas, *On Towers and Composita of Towers of Function Fields over Finite Fields*, Finite Fields and their Applications 3, 1997, 257-274.

[Gee-Vlu 1] G. van der Geer, M. van der Vlugt, *Tables of Curves with Many Points*, http://www.wins.uva.nl/~geer.

[Gee-Vlu 2] G. van der Geer, M. van der Vlugt, *Kummer Covers with Many Points*, Finite Fields and their Applications 6, 2000, 327-342.

[Gop] V. D. Goppa, *Codes on Algebraic Curves*, Sov. Math.-Dokl. 24, 1981, 170-172.

[Grä] H.-G. Gräbe, *Grundlegende Algorithmen der Computeralgebra*, http://www.informatik.uni-leipzig.de/~graebe.

[Hac] G. Haché, *Construction effective des codes géométriques*, Ph. D. Dissertation, Université Paris 6, France, 1996.

[Knu 1] D. E. Knuth, *The Art of Computer Programming, Fundamental Algorithms*, Vol. 1, Reading, Mass.: Addison-Wesley 1969.

[Knu 2] D. E. Knuth, *The Art of Computer Programming, Seminumerical Algorithms*, Vol. 2, Reading, Mass.: Addison-Wesley 1969.

[Knu 3] D. E. Knuth, *The Art of Computer Programming, Sorting and Searching*, Vol. 3, Reading, Mass.: Addison-Wesley 1969.

[Leo] D. A. Leonard *Finding the Defining Functions for the One-Point AG-Codes*, IEEE Trans. Information Theory 47, 2001, 2566-2573.

[Pel-Sti-Tor] R. Pellikaan, H. Stichtenoth, F. Torres *Weierstrass Semigroups in an Asymptotically Good Tower of Function Fields*, Finite Fields and their Applications 4, 1998, 381-392.

[Rab] M. O. Rabin *Probabilistic Algorithms in Finite Fields*, SIAM J. Comp. 9, 1980, 273-280.

[Sha-Bee] Y. Shany and Y. Be'ery, *Towards the Construction of Codes on the First Garcia-Stichtenoth Tower of Function Fields*, Tel-Aviv University, Israel, 2001, E-mail: {shany,ybeery}@eng.tau.ac.il.

[Shu-Ale-Kum-Sti-Deo] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, V. Deolalikar, *A Low-Complexity Algorithm for the Construction of Algebraic-Geometric Codes Better Than the Gilbert-Varshamov Bound*, IEEE Trans. Information Theory 47, 2001, 2225-2241.

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag Berlin-Heidelberg 1993.

[Tho] M. Thomas, *Türme und Pyramiden algebraischer Funktionenkörper*, Dissertation, Universität Essen, 1997.

[Tsf-Vla-Zin] M. A. Tsfasman, S. G. Vlădut, T. Zink, *Modular Curves, Shimura Curves, and Goppa Codes, Better Than Varshamov-Gilbert Bound*, Math. Nachr. 109, 1982, 21-28.

[Vos-Høh] C. Voss, T. Høholdt, *An Explicit Construction of a Sequence of Codes Attaining the Tsfasman-Vlădut-Zink Bound: The First Steps*, IEEE Trans. Information Theory 43, 1997, 128-135.